BT

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION T

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006590 A2

(51) International Patent Classification[7]: H04Q

(21) International Application Number: PCT/US2003/021280

(22) International Filing Date: 8 July 2003 (08.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/192,488	9 July 2002 (09.07.2002)	US
60/396,577	16 July 2002 (16.07.2002)	US
10/318,432	13 December 2002 (13.12.2002)	US

(71) Applicant: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.** [US/US]; American Express Tower, World Financial Center, New York City, NY 10285-4900 (US).

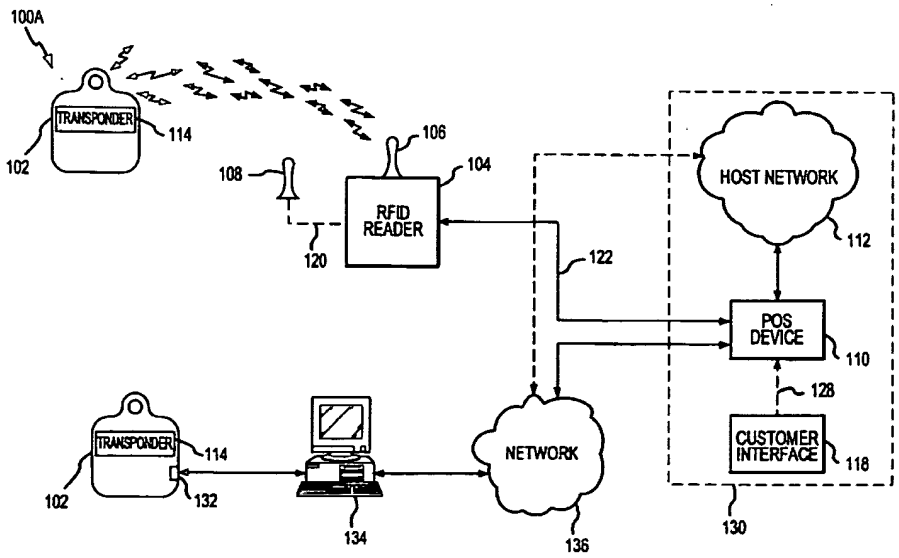
(72) Inventors: **BERARDI, Michael, J.**; 770 NW 50th Street, #306, Ft. Lauderdale, FL 33351 (US). **BLIMAN, Michal**; 4 Dogwood Circle, Matawan, NJ 07747 (US). **BONALLE, David**; 77 Rose Hill Avenue, New Rochelle, NY 10804 (US). **ELWOOD, Jennifer, A.**; 245 East 84th Street, #3E, New York City, NY 10028 (US). **HOOD, Matthew, C.**; 1112 LaFayette Road, Wayne, PA 19087 (US). **ISENBERG, Susan, E.**; 201 West 74th, #12H, New York City, NY 10023 (US). **MAYERS, Alexandra**; 49 Grove Street, #5B, New York City, NY 10014 (US). **PERRY, Trevor, J.**; 2554 West 6300 South, West Jordan, UT 84084 (US). **SAUNDERS, Peter, D.**; 3710 East Palisade Drive, Salt Lake City, UT 84109 (US). **SCHEDING, Kathryn, D.**; 220 East 54th Street, #6J, New York City, NY 10022 (US). **SHAH, Sejal, Ajit**; 30 West 63rd, #21E, New York City, NY 10023 (US). **VONWALD, Kristin, L.**; 1236 Man of War Cove, South Jordan, Ut 84095 (US). **WILLIAMSON, John, R.**; 302 Pavonia Avenue, Jersey City, NJ 07302 (US).

(74) Agent: **SOBELMAN, Howard, I.**; Snell & Wilmer, L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SELECTING LOAD OPTIONS FOR USE IN RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS



(57) Abstract: A transponder-reader payment system includes a fob including a transponder, and a RFID reader for interrogating the transponder. In exemplary operation, the fob identifying information may be presented to the RFID reader for completion of a transaction request. The transaction request may be provided to a fob issuer system which retrieves a value for satisfying the transaction request from a fob associated transaction data file. The issuer system may deplete the transaction data file in accordance with the transaction request and replenish the data file in accordance with fob user or fob issuer defined reload protocol.

WO 2004/006590 A2

SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SELECTING LOAD OPTIONS FOR USE IN RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS

Field of Invention

This invention generally relates to a system and method for completing a transaction, and more particularly, to determining the loading criteria for a funding source associated with a Radio Frequency Identification (RFID) device used in completing a financial transaction.

Background of the Invention

Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in completing financial transactions. A typical fob includes a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder. In which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independently of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal. U.S. Patent No. 5,053,774 issued to Schuermann describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional

transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

In the conventional fob powering technologies used, the fob is typically activated upon presenting the fob in an interrogation signal. In this regard, the fob may be activated irrespective of whether the user desires such activation. Inadvertent presentation of the fob may result in initiation and completion of an unwanted transaction. Thus, a fob system is needed which allows the fob user to control activation of the fob to limit transactions being undesirably completed.

One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point of Sale (POS) device. Fob identification data is typically passed to a third party server database, where the identification data is referenced to a customer (*e.g.*, user) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to an authorizing entity. Once authorization is received by the server, clearance is sent to the point of sale device for completion of the transaction. In this way, the conventional transaction processing method involves an indirect path which causes undue overhead due to the use of the third-party server.

A need exists for a transaction authorization system which allows fob transactions to be authorized while eliminating the cost associated with using third-party servers.

In addition, conventional fobs are limited in that they must be used in proximity to the Point of Sale device. That is, for fob activation, conventional fobs must be positioned within the area of transmission cast by the RF interrogation signal. More particularly, conventional fobs are not affective for use in situations where the user wishes to conduct a transaction at a point of interaction such as a computer interface.

Therefore, a need exists for a fob embodying RFID acquisition technology, which is capable of use at a point of interaction device and which is additionally capable of facilitating transactions via a computer interface connected to a network (*e.g.*, the Internet).

Existing transponder-reader payment systems are also limited in that the conventional fob used in the systems is only responsive to one interrogation signal. Where multiple interrogation signals are used, the fob is only responsive to the interrogation signal to which it is configured. Thus, if the RFID reader of the system provides only an interrogation signal to which the fob is incompatible, the fob will not be properly activated.

Therefore, a need exists for a fob which is responsive to more than one interrogation signal.

Existing transponder-reader payment systems are additionally limited in that the payment systems are typically linked to a funding source with a predetermined spending limit. Thus no flexibility is provided in instances where the payment is requested which exceeds the predetermined spending limit. This is typically true since traditional methods for processing a requested transaction involve comparing the transaction to the spending limit or to an amount stored in a preloaded value data file prior to providing transaction authorization to a merchant.

Thus, a system is needed which processes transponder-reader payment requests without comparing the amount of the request to the amount available from the transponder-reader payment system funding source or associated fob account data file.

Further, traditional transponder-reader systems do not permit the user to manage the system user account data. This is extremely problematic where the user wishes to change a transponder-reader system funding source to a source which provides more available spending room, or where changes are made to user's status (*e.g.*, change in address, phone number, email, etc.) for which the transponder-reader account provider wishes to readily update the user's account.

Thus a need exists for a transponder-reader system which will allow the user limited access to the transponder-reader account for managing account data.

Further still, existing transponder-reader systems do not permit means for automatically incenting the use of the fob associated with the system as opposed to the credit or charge card associated with the fob. That is, conventional transponder-reader systems do not provide a means for encouraging usage of the transponder reader system by encouraging use of the fob product since the present

systems do not distinguish between usage of a system transponder and a charge or credit card account associated with the transponder.

Consequently, a need exists for a transponder-reader system which is capable of determining when a system transponder is used, and incenting such usage.

Sill further, present systems are limited in that the systems are unable to track credit or charge card usage and fob usage for a single funding source. For example, in typical prior art systems, a fob may be linked to a specified funding source (*e.g.*, American Express, MasterCard, Visa, etc.) which may be used to provide funds for satisfaction of a transaction request. The funding source may additionally have a consumer credit or charge card which may be associated with the fob and which may be used for contact transactions. Where the credit or charge card is used, a statement reporting the card usage is provided to the card user. However, the reporting statement does not include a reporting of the fob product usage. Thus, a fob user is unable to chart, analyze or compare fob usage to the usage of the associated card. This is especially problematic where the funding source is used by more than one entity (*e.g.*, spouses, multiple company personnel, etc.) where one entity may use the fob and a separate entity may use the card associated with the fob.

Thus, a need exists for a transponder-reader payment system which would permit reporting of the fob usage and the credit card usage in a single file.

Summary of the Invention

Described herein is a system and method for using RFID technology to initiate and complete financial transactions. The transponder-reader payment system described herein may include a RFID reader operable to provide a RF interrogation signal for powering a transponder system, receiving a transponder system RF signal, and providing transponder system account data relative to the transponder system RF signal. The transponder-reader payment system may include a RFID protocol/sequence controller in electrical communication with one or more interrogators for providing an interrogation signal to a transponder, a RFID authentication circuit for authenticating the signal received from the transponder, a serial or parallel interface for interfacing with a point of interaction device, and an

USB or serial interface for use in personalizing the RFID reader and/or the transponder. The transponder-reader payment system may further include a fob including one or more transponders (*e.g.*, modules) responsive to one or more interrogation signals and for providing an authentication signal for verifying that the transponder and/or the RFID reader are authorized to operate within the transponder-reader payment system. In this way, the fob may be responsive to multiple interrogation signals provided at different frequencies. Further, the fob may include a USB or serial interface for use with a computer network or with the RFID reader.

The RFID system and method according to the present invention may include a transponder which may be embodied in a fob, tag, card or any other form factor (*e.g.*, wristwatch, keychain, cell phone, etc.), which may be capable of being presented for interrogation. In that regard, although the transponder is described herein as embodied in a fob, the invention is not so limited.

The system may further include a RFID reader configured to send a standing RFID recognition signal which may be transmitted from the RFID reader via radio frequency (or electromagnetic) propagation. The fob may be placed within proximity to the RFID reader such that the RFID signal may interrogate the fob and initialize fob identification procedures.

In one exemplary embodiment, as a part of the identification process, the fob and the RFID reader may engage in mutual authentication. The RFID reader may identify the fob as including an authorized system transponder for receiving encrypted information and storing the information on the fob memory. Similarly, the fob, upon interrogation by the RFID reader, may identify the RFID reader as authorized to receive the encrypted and stored information. Where the RFID reader and the fob successfully mutually authenticate, the fob may transmit to the RFID reader certain information identifying the transaction account or accounts to which the fob is associated. The RFID reader may receive the information and forward the information to facilitate the completion of a transaction. In one exemplary embodiment, the RFID reader may forward the information to a point of interaction device (*e.g.*, POS or computer interface) for transaction completion. The mutual authorization process disclosed herein aids in ensuring fob transponder-reader payment system security.

In another exemplary embodiment, the fob according to the present invention, includes means for completing transactions via a computer interface. The fob may be connected to the computer using a USB or serial interface fob account information may be transferred to the computer for use in completing a transaction via a network (*e.g.*, the Internet).

In yet another exemplary embodiment of the present invention, a system is provided which incents usage of the transponder-reader system transponder (*e.g.*, fob). The system distinguishes between the usage of a fob and the usage of a charge or credit card sharing the same funding source as the fob. Where the fob is used, the system may provide reward points to the user based on criteria predetermined by the issuer. Additionally, where a preloaded fob system is used, the present invention recognizes when the associated fob preloaded value data file is loaded or reloaded with funds. The invention then may provide reward points based on the criteria associated with the loading or reloading action. Further, the system according to this invention may incent patronage of a merchant. In this case, the system may receive a fob transaction request and incent the fob user based on a marker or other identifying indicia correlated with the merchant. The marker may be included in the transaction identification, in a merchant identification provided with the transaction, or a combination of both.

In still another exemplary embodiment of the invention, a system is disclosed which permits the user to manage the account associated with the fob. The user is provided limited access to the fob account information stored on the account provider database for updating, for example, demographic information, account funding source, and/or account restrictions (*e.g.*, spending limits, personal identification number, etc.). Access to the account may be provided to the user telephonically or via a network (*e.g.*, online).

In yet another exemplary embodiment, a system permitting fob user access to manage the fob account permits the user to indicate loading, preloading and reloading value amounts for a preloaded data file or funding account. The fob user may be permitted access to a fob account provider (*e.g.* "issuer") database for identifying a reload protocol which would indicate an initial amount for a preloaded funding source, the funding source from which to reload, the reloading frequency, whether reloading should be automatic or manual, and a decision flow for reloading

based on merchant, type of transaction, or the like. The preloaded funding source may be any funding source associated with the fob, which contains value stored in a preloaded value data file redeemable during a merchant transaction request. The value amount contained in the preloaded value data file may be balanced against a merchant transaction request and depleted according to the transaction request. Consequently, the preloaded value data file may become depleted where the total value of the transaction request is equal to the value stored in the preloaded value data file.

The system permits the fob user to automatically or manually reload the preloaded value data file to a specified value according to a predetermined criteria. The fob user may be permitted to access fob account information maintained on a issuer system (or access any other system which can facilitate access or changes), and establish on the issuer system a load/reload protocol for the fob account. The fob user may define that the fob preloaded value data file (e.g., "preload account") may be loaded or reloaded according to a pre-identified merchant or class of transactions, etc. Where the fob user is completing a transaction on line, the fob user may be notified that a particular merchant transaction involves loading or that a merchant requests a particular funding source. Such notification may be in real-time, and the fob user may be permitted to indicate reloading of the preloaded value data file prior to completion of a transaction.

In a further exemplary embodiment, the present invention provides methods for processing a transaction request whereby the amount of the transaction request may be approved prior to requesting funding from the funding source and/or verifying that the amount for completing the transaction is available. In this way, the transaction may be approved provided the transaction and/or account meets certain predetermined authorization criteria. Once the criteria is met, the transaction is authorized and authorization is provided to the requesting agent (*e.g.*, merchant). In one instance the payment for the transaction is requested from the funding source simultaneously to, or immediately following, the providing of the authorization to the merchant. In another instance the payment for transactions is requested at a time period later than when the authorization is provided to the merchant.

These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

Brief Description of the Drawings

The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

FIG. 1A illustrates an exemplary RFID-based system in accordance with the present invention, wherein exemplary components used for fob transaction completion are depicted;

FIG. 1B illustrates an exemplary personalization system in accordance with the present invention;

FIG. 2 is a schematic illustration of an exemplary fob in accordance with the present invention;

FIG. 3 is a schematic illustration of an exemplary RFID reader in accordance with the present invention;

FIG. 4 is an exemplary flow diagram of an exemplary authentication process in accordance with the present invention;

FIG. 5 is an exemplary flow diagram of an exemplary decision process for a protocol/sequence controller in accordance with the present invention;

FIGS. 6A-B are an exemplary flow diagram of a fob personalization process in accordance with the present invention;

FIGS. 7A-B are an exemplary flow diagram of a RFID reader personalization process in accordance with the present invention;

FIG. 8 is a flow diagram of an exemplary payment/transaction process in accordance with the present invention;

FIG. 9 is another schematic illustration of an exemplary fob in accordance with the present invention;

FIG. 10 is a depiction of an exemplary preloaded fob payment/transaction process in accordance with the present invention;

FIGs. 11A-B are a depiction of an exemplary preloaded fob account reload process in accordance with the present invention;

FIG. 12 is a depiction of an exemplary Direct Link payment/transaction process in accordance with the present invention; and

FIG. 13 is a depiction of another exemplary payment/transaction process in accordance with the present invention.

Detailed Description

The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components, *e.g.*, memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more mircroprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®, Blueberry®), cellular phone and/or the like.

Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

FIG. 1A illustrates an exemplary RFID transaction system 100A in accordance with the present invention, wherein exemplary components for use in completing a fob transaction are depicted. In general, the operation of system 100A may begin when fob 102 is presented for payment, and is interrogated by RFID reader 104 or, alternatively, interface 134. Fob 102 and RFID reader 104 may then engage in mutual authentication after which the transponder 102 may provide the transponder identification and/or account identifier to the RFID reader 104 which may further provide the information to the merchant system 130 POS device 110.

System 100A may include a fob 102 having a transponder 114 and a RFID reader 104 in RF communication with fob 102. Although the present invention is described with respect to a fob 102, the invention is not to be so limited. Indeed, system 100 may include any device having a transponder which is configured to communicate with a RFID reader 104 via RF communication. Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

The RFID reader 104 may be configured to communicate using a RFID internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 for communications with fob 102, where the external antenna may be made remote to the RFID reader 104 using a suitable cable and/or data link 120. RFID reader 104 may be further in communication with a merchant system 130 via a data link 122. The system 100A may include a transaction completion system including a point of interaction device such as, for example, a merchant point of sale (POS) device 110 or a computer interface (*e.g.*, user interface) 134. In one

exemplary embodiment the transaction completion system may include a merchant system 130 including the POS device 110 in communication with a RFID reader 104 (via data link 122). As described more fully below, the transaction completion system may include the user interface 134 connected to a network 136 and to the transponder via a USB connector 132.

Although the point of interaction device is described herein with respect to a merchant point of sale (POS) device, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point of interaction device may be any device capable of receiving fob account data. In this regard, the POS may be any point of interaction device enabling the user to complete a transaction using a fob 102. POS device 110 may be in further communication with a customer interface 118 (via data link 128) for entering at least a customer identity verification information. In addition, POS device 110 may be in communication with a merchant host network 112 (via data link 124) for processing any transaction request. In this arrangement, information provided by RFID reader 104 is provided to the POS device 110 of merchant system 130 via data link 122. The POS device 110 may receive the information (and alternatively may receive any identity verifying information from customer interface 118 via data link 128) and provide the information to host system 112 for processing.

A variety of conventional communications media and protocols may be used for data links 120, 122, 124, and 128. For example, data links 120, 122, 124, and 128 may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system 130 including the POS device 110 and host network 112 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The merchant system 130 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

An account number, as used herein, may include any identifier for an account (*e.g.*, credit, charge debit, checking, savings, reward, loyalty, or the like) which may be maintained by a transaction account provider (*e.g.*, payment authorization center) and which may be used to complete a financial transaction. A typical account number (*e.g.*, account data) may be correlated to a credit or debit account, loyalty account, or rewards account maintained and serviced by such entities as American Express®, Visa® and/or MasterCard® or the like. For ease in understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

In addition, the account number (*e.g.*, account data) may be associated with any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other identification indicia. The account number may be optionally located on a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data to a second device. A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express®. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and, etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to fob 102. In one exemplary embodiment, the account number may include a unique fob serial number and user

identification number, as well as specific application applets. The account number may be stored in fob 102 inside a database 214, as described more fully below. Database 214 may be configured to store multiple account numbers issued to the fob 102 user by the same or different account providing institutions. Where the account data corresponds to a loyalty or rewards account, the database 214 may be configured to store the attendant loyalty or rewards points data.

FIG. 2 illustrates a block diagram of the many functional blocks of an exemplary fob 102 in accordance with the present invention. Fob 102 may be a RFID fob 102 which may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of example, the fob 102 may be a RFID fob which may be presented for facilitating payment for goods and/or services.

Fob 102 may include an antenna 202 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Fob antenna 202 may be in communication with a transponder 114. In one exemplary embodiment, transponder 114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 202 may be of the 13 MHz variety. The transponder 114 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 114 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 206 may be configured to format (*e.g.*, demodulate) a signal received from the later connected circuitry in a format compatible with transponder 114 for transmitting to RFID reader 104 via antenna 202. For example, where transponder 114 is of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

Modulator/demodulator 206 may be coupled to a protocol/sequence controller 208 for facilitating control of the authentication of the signal provided by RFID reader 104, and for facilitating control of the sending of the fob 102 account number. In this regard, protocol/sequence controller 208 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the fob 102 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by the RFID

reader 104 is authenticated, and thereby providing to the RFID reader 104 the account number stored on fob 102.

Protocol/sequence controller 208 may be further in communication with authentication circuitry 210 for facilitating authentication of the signal provided by RFID reader 104. Authentication circuitry may be further in communication with a non-volatile secure memory database 212. Secure memory database 212 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. Database 212 may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, NY), any of the database products available from Oracle Corporation (Redwood Shores, CA), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Database 212 may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

The data may be used by protocol/sequence controller 208 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry may authenticate the signal provided by RFID reader 104 by association of the RFID signal to authentication keys stored on database 212.

Encryption circuitry may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from the RFID reader 104.

In addition, protocol/sequence controller 208 may be in communication with a database 214 for storing at least a fob 102 account data, and a unique fob 102 identification code. Protocol/sequence controller 208 may be configured to retrieve the account number from database 214 as desired. Database 214 may be of the same configuration as database 212 described above. The fob account data and/or unique fob identification code stored on database 214 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique fob identification code from database 214, the account number may be encrypted when being provided to RFID reader 104. Further, the data stored on database 214 may include, for example, an unencrypted unique fob 102 identification code, a user identification, Track 1 and 2 data, as well as specific application applets.

Fob 102 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 104. That is, as described more fully below, RFID reader 104 may provide more than one RF interrogation signal. In this case, fob 102 may be configured to respond to the multiple frequencies by including in fob 102 one or more additional RF signal receiving/transmitting units 226. RF signal receiving/transmitting unit 226 may include an antenna 218 and transponder 220 where the antenna 218 and transponder 220 are compatible with at least one of the additional RF signals provided by RFID reader 104. For example, in one exemplary embodiment, fob 102 may include a 134 KHz antenna 218 configured to communicate with a 134 KHz transponder 220. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 KHz transponder may be configured to communicate directly with the protocol/sequence controller 208 for transmission and receipt of authentication and account number signals as described above.

In another embodiment, fob 102 may further include a universal serial bus (USB) connector 132 for interfacing fob 102 to a user interface 134. User interface 134 may be further in communication with a POS device 110 via a network 136. Network 136 may be the Internet, an intranet, or the like as is described above with respect to network 112. Further, the user interface 134 may be similar in

construction to any conventional input devices and/or computing systems aforementioned for permitting the system user to interact with the system. In one exemplary embodiment, fob 102 may be configured to facilitate online Internet payments. A USB converter 222 may be in communication with a USB connector 232 for facilitating the transfer of information between the modulator/demodulator 206 and USB connector 132. Alternatively, USB converter 222 may be in communication with protocol/sequence controller 208 to facilitate the transfer of information between protocol/sequence controller 208 and USB connector 132.

Where fob 102 includes a USB connector 132, fob 102 may be in communication with, for example, a USB port on user interface 134. The information retrieved from fob 102 may be compatible with credit card and/or smart card technology enabling usage of interactive applications on the Internet. No RFID reader may be required in this embodiment since the connection to POS device 110 may be made using a USB port on user interface 134 and a network 136.

Fob 102 may include means for enabling activation of the fob by the user. In one exemplary embodiment, a switch 230 which may be operated by the user of the fob 102. The switch 230 on fob 102 may be used to selectively or inclusively activate the fob 102 for particular uses. In this context, the term "selectively" may mean that the switch 230 enables the user to place the fob 102 in a particular operational mode. For example, the user may place the fob 102 in a mode for enabling purchase of a good or of a service using a selected account number. Alternatively, the fob may be placed in a mode as such that the fob account number is provided by USB port 132 (or serial port) only and the fob transponder 114 is disabled. In addition, the term "inclusively" may mean that the fob 102 is placed in an operational mode permitting the fob 102 to be responsive to the RF interrogation and interrogation via the USB connector 132. In one particular embodiment, the switch 230 may remain in an OFF position ensuring that one or more applications or accounts associated with the fob 102 are non-reactive to any commands issued by RFID reader 104. As used herein, the OFF position may be termed the "normal" position of the activation switch 230, although other normal positions are contemplated.

In another exemplary embodiment, when the switch 230 is moved from the OFF position, the fob 102 may be deemed activated by the user. That is, the switch

230 may activate internal circuitry in fob 102 for permitting the fob to be responsive to RF signals (*e.g.*, commands from RFID reader 104). In this way, switch 230 may facilitate control of the active and inactive states of the fob 102. Such control increases the system security by preventing inadvertent or illegal use of the fob 102.

In one exemplary embodiment, switch 230 may be a simple mechanical device in communication with circuitry which may electrically prevent the fob from being powered by a RFID reader. That is, when switch 230 is in its normal position, switch 230 may provide a short to the fob 102 internal circuitry, preventing fob 102 from being responsive to interrogation by RF or via the USB connector 230. In this arrangement, the switch 230 may be, for example, a "normally closed" (NC) configured switch, which may be electrically connected to the antenna 202 at the interface of the antenna 202 and the transponder 114. The switch 230 may be depressed, which may open the switch 230 fully activating the antenna 202.

In yet another exemplary embodiment, the fob 102 may include a biometric sensor and biometric membrane configured to operate as switch 230 and activate the fob 102 when provided biometric signal from the fob 102 user. Such biometric signal may be the digital reading of a fingerprint, thumbprint, or the like. Typically, where biometric circuitry is used, the biometric circuitry may be powered by an internal voltage source (*e.g.*, battery). In this case, the switch may not be a simple mechanical device, but a switch which is powered. In yet another exemplary embodiment, switch 230 may be battery powered though no biometric circuitry is present in the fob 102.

In yet another embodiment, the switch 230 may be a logic switch. Where switch 230 is a logic switch the switch 230 control software may be read from the sequence controller 208 to selectively control the activation of the various fob 102 components.

FIG. 3 illustrates an exemplary block diagram of a RFID reader 104 in accordance with an exemplary embodiment of the present invention. RFID reader 104 includes, for example, an antenna 106 coupled to a RF module 302, which is further coupled to a control module 304. In addition, RFID reader 104 may include an antenna 108 positioned remotely from the RFID reader 104 and coupled to RFID reader 104 via a suitable cable 120, or other wire or wireless connection.

RF module 302 and antenna 106 may be suitably configured to facilitate communication with fob 102. Where fob 102 is formatted to receive a signal at a particular RF frequency, RF module 302 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 102 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 106 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 102 may be configured to include a first and second RF module (*e.g.*, transponder) where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. The RFID reader 104 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 104 is operating at 134 kHz frequency, only operation with the 134 kHz module on the fob 102 may be possible. When the reader 104 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on the fob 102 may be possible. Where the reader 104 supports both a 134 kHz frequency and a 13.56 MHz RF module, the fob 102 may receive both signals from the reader 104. In this case, the fob 102 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, the reader 104 may receive signals at both frequencies from the fob upon interrogation. In this case, the reader 104 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

Further, protocol/sequence controller 314 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform the fob 102 user that the transaction is initiated (*e.g.*, fob is being interrogated), the fob is valid (*e.g.*, fob is authenticated), transaction is being processed, (*e.g.*, fob account number is being read by RFID reader) and/or the transaction is accepted or denied (*e.g.*, transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing the fob 102 user of the transaction status. The audible feedback may be a simple tone,

multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 102 is being interrogated, the transaction status, or the like.

RFID antenna 106 may be in communication with a transponder 306 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 102. Transponder 306 may be of similar description as transponder 114 of FIG. 2. In particular, transponder 306 may be configured to send and/or receive RF signals in a format compatible with antenna 202 in similar manner as was described with respect to fob transponder 114. For example, where transponder 306 is 13.56 MHz RF rated antenna 202 may be 13.56 MHz compatible. Similarly, where transponder 306 is ISO/IEC 14443 rated, antenna 106 may be ISO/IEC 14443 compatible.

RF module 302 may include, for example, transponder 306 in communication with authentication circuitry 308 which may be in communication with a secure database 310. Authentication circuitry 308 and database 310 may be of similar description and operation as described with respect to authentication circuitry 210 and secure memory database 212 of FIG. 2. For example, database 310 may store data corresponding to the fob 102 which are authorized to transact business over system 100. Database 310 may additionally store RFID reader 104 identifying information for providing to fob 102 for use in authenticating whether RFID reader 104 is authorized to be provided the fob account number stored on fob database 214.

Authentication circuitry 308 may be of similar description and operation as authentication circuitry 210. That is, authentication circuitry 308 may be configured to authenticate the signal provided by fob 102 in similar manner that authentication circuitry 210 may be configured to authenticate the signal provided by RFID reader 104. As is described more fully below, fob 102 and RFID reader 104 engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until fob 102 authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from fob 102.

Fig. 4 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the

fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

As noted, database 212 may store security keys for encrypting or decrypting signals received from RFID reader 104. In an exemplary authentication process, where RFID reader 104 is authenticating fob 102, RFID reader 104 may provide an interrogation signal to fob 102 (step 402). The interrogation signal may include a random code generated by the RFID reader authentication circuit 210, which is provided to the fob 102 and which is encrypted using an unique encryption key corresponding to the fob 102 unique identification code. For example, the protocol/sequence controller 314 may provide a command to activate the authentication circuitry 308. Authentication circuitry 308 may provide from database 310 a fob interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (*e.g.*, readable) by the RFID reader 104 and the fob 102. The authentication code may be provided to the fob 102 via the RFID RF interface 306 and antenna 106 (or alternatively antenna 108).

Fob 102 receives the interrogation signal (step 404). The interrogation signal including the authorization code may be received at the RF interface 114 via antenna 202. Once the fob 102 is activated, the interrogation signal including the authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence controller 208. Protocol/sequence controller 208 may recognize the interrogation signal as a request for authentication of the fob 102, and provide the authentication code to authentication circuit 210. The fob 102 may then encrypt the authentication code (step 406). In particular, encryption may be done by authentication circuit 210, which may receive the authentication code and encrypt the code prior to providing the encrypted authentication code to protocol/sequence controller 208. Fob 102 may then provide the encrypted authentication code to the RFID reader 104 (step 408). That is, the encrypted authentication code may be provided to the RFID reader 104 via modulator/demodulator circuit 206, RF interface 114 (*e.g.*, transponder 114) and antenna 202.

RFID reader 104 may then receive the encrypted authentication code and decryption it (step 410). That is, the encrypted authentication code may be received at antenna 106 and RF interface 306 and may be provided to authentication circuit 308. Authentication circuit 308 may be provided a security authentication key (*e.g.*, transponder system decryption key) from database 310. The authentication circuit may use the authentication key to decrypt (*e.g.*, unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit based on the fob 102 unique identification code. For example, the encrypted authentication code may be provided along with the unique fob 102 identification code. The authentication circuit may receive the fob 102 unique identification code and retrieve from the database 310 a transponder system decryption key correlative to the unique fob 102 identification code for use in decrypting the encrypted authentication code.

Once the authentication code is decrypted, the decrypted authentication code is compared to the authentication code provided by the RFID reader 104 at step 402 (step 412) to verify its authenticity. If the decrypted authorization code is not readable (*e.g.*, recognizable) by the authentication circuit 308, the fob 102 is deemed to be unauthorized (*e.g.*, unverified) (step 416) and the operation of system 100 is terminated (step 418). Contrarily, if the decrypted authorization code is recognizable (*e.g.*, verified) by the fob 102, the decrypted authorization code is deemed to be authenticated (step 412), and the transaction is allowed to proceed (step 414). In one particular embodiment, the proceeding transaction may mean that the fob 102 may authenticate the RFID reader 104 prior to the RFID reader 104 authenticating fob 102, although, it should be apparent that the RFID reader 104 may authenticate the fob 102 prior to the fob 102 authenticating the RFID reader 104.

It should be noted that in an exemplary verification process, the authorization circuit 308 may determine whether the unlocked authorization code is identical to the authorization code provided in step 402. If the codes are not identical then the fob 102 is not authorized to access system 100. Although, the verification process is described with respect to identicality, identicality is not required. For example, authentication circuit 308 may verify the decrypted code through any protocol,

steps, or process for determining whether the decrypted code corresponds to an authorized fob 102.

Authentication circuitry 308 may additionally be in communication with a protocol/sequence controller 314 of similar operation and description as protocol/sequence controller 208 of FIG. 2. That is, protocol/sequence device controller 314 may be configured to determine the order of operation of the RFID reader 104 components. For example, FIG. 5 illustrates and exemplary decision process under which protocol/sequence controller 314 may operate. Protocol/sequence controller 314 may command the different components of RFID reader 104 based on whether a fob 102 is present (step 502). For example, if a fob 102 is not present, then protocol/sequence controller 314 may command the RFID reader 104 to provide an uninterrupted interrogation signal (step 504). That is, the protocol/sequence controller may command the authentication circuit 308 to provide an uninterrupted interrogation signal until the presence of a fob 102 is realized. If a fob 102 is present, the protocol/sequence controller 314 may command the RFID reader 104 to authenticate the fob 102 (step 506).

As noted above, authentication may mean that the protocol/sequence controller 314 may command the authentication circuit 308 to provide fob 102 with an authorization code. If a response is received from fob 102, protocol/sequence controller may determine if the response is a response to the RFID reader 104 provided authentication code, or if the response is a signal requiring authentication (step 508). If the signal requires authentication, then the protocol/sequence controller 314 may activate the authentication circuit as described above (step 506). On the other hand, if the fob 102 signal is a response to the provided authentication code, then the protocol/sequence controller 314 may command the RFID reader 104 to retrieve the appropriate security key for enabling recognition of the signal (step 510). That is, the protocol/sequence controller 314 may command the authentication circuit 308 to retrieve from database 310 a security key (*e.g.*, transponder system decryption key), unlock the signal, and compare the signal to the signal provided by the RFID reader 104 in the authentication process (*e.g.*, step 506). If the signal is recognized, the protocol/sequence controller 314 may determine that the fob 102 is authorized to access the system 100. If the signal is not recognized, then the fob 102 is considered not authorized. In which case, the

protocol/sequence controller 314 may command the RFID controller to interrogate for authorized fobs (step 504).

Once the protocol/sequence controller determines that the fob 102 is authorized, the protocol/sequence controller 314 may seek to determine if additional signals are being sent by fob 102 (step 514). If no additional signal is provided by fob 102, then the protocol/sequence controller 314 may provide all the components of RFID reader 104 to remain idle until such time as a signal is provided (step 516). Contrarily, where an additional fob 102 signal is provided, the protocol/sequence controller 314 may determine if the fob 102 is requesting access to the merchant point of sale terminal 110 (*e.g.*, POS device) or if the fob 102 is attempting to interrogate the RFID reader 104 for return (*e.g.*, mutual) authorization (step 518). Where the fob 102 is requesting access to a merchant point of sale terminal 110, the protocol/sequence controller 314 may command the RFID reader 104 to open communications with the point of sale terminal 110 (step 524). In particular, the protocol/sequence controller 314 may command the point of sale terminal communications interface 312 to become active, permitting transfer of data between the RFID reader 104 and the merchant point of sale terminal 110.

On the other hand, if the protocol/sequence controller determines that the fob 102 signal is a mutual interrogation signal, then the protocol/sequence controller may command the RFID reader 104 to encrypt the signal (step 520). The protocol/sequence controller 314 may command the encryption authentication circuit 318 to retrieve from database 320 the appropriate encryption key in response to the fob 102 mutual interrogation signal. The protocol/sequence controller 314 may then command the RFID reader 104 to provide the encrypted mutual interrogation signal to the fob 102. The protocol/sequence controller 314 may command the authentication circuit 318 to provide an encrypted mutual interrogation signal for the fob 102 to mutually authenticate. Fob 102 may then receive the encrypted mutual interrogation signal and retrieve from authentication circuitry 212 a RFID reader decryption key.

Although an exemplary decision process of protocol/sequence controller 314 is described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 208 in controlling the components of fob 102. Indeed, as described above, protocol/sequence controller 314 may have

similar operation and design as protocol/sequence controller 208. In addition, to the above, protocol/sequence controllers 208 and 314 may incorporate in the decision process appropriate commands for enabling USB interfaces 222 and 316, when the corresponding device is so connected.

Encryption/decryption component 318 may be further in communication with a secure account number database 320 which stores the security keys necessary for decrypting the encrypted fob account number. Upon appropriate request from protocol/sequence controller 314, encryption/decryption component (*e.g.*, circuitry 318) may retrieve the appropriate security key, decrypt the fob account number and forward the decrypted account number to protocol sequence controller 314 in any format readable by any later connected POS device 110. In one exemplary embodiment, the account number may be forwarded in a conventional magnetic stripe format compatible with the ISO/IEC 7813 standard. Upon receiving the account number in magnetic stripe format, protocol/sequence controller 314 may forward the account number to POS device 110 via a communications interface 312 and data link 122, as best shown in Figure 1. POS device 110 may receive the decrypted account number and forward the magnetic stripe formatted account number to a merchant network 112 for processing under the merchant's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where the POS device 110 receives a response from network 112 (*e.g.*, transaction authorized or denied), protocol/sequence controller 314 may provide the network response to the RF module 302 for optically and/or audibly communicating the response to the fob 102 user.

RFID reader 104 may additionally include a USB interface 316, in communication with the protocol/sequence controller 314. In one embodiment, the USB interface may be a RS22 serial data interface. Alternatively, the RFID reader 104 may include a serial interface such as, for example, a RS232 interface in communication with the protocol/sequence controller 314. The USB connector 316 may be in communication with a personalization system 116 (shown in FIG. 1B) for initializing RFID reader 104 to system 100 application parameters. That is, prior to operation of system 100, RFID reader 104 may be in communication with personalization system 116 for populating database 310 with a listing of security keys belonging to authorized fobs 102, and for populating database 320 with the

security keys to decrypt the fob 102 account numbers placing the account numbers in ISO/IEC 7813 format. In this way, RFID reader 104 may be populated with a unique identifier (*e.g.*, serial number) which may be used by fob authentication circuitry 210 to determine if RFID reader 104 is authorized to receive a fob 102 encrypted account number.

FIG. 1B illustrates an exemplary personalization system 100B, in accordance with the present invention. In general, typical personalization system 100B may be any system for initializing the RFID reader 104 and fob 102 for use in system 100A. With reference to FIG. 1B, the similar personalization process for fob 102 may be illustrated. For example, personalization system 116 may be in communication with fob 102 via RF ISO 14443 interface 114 for populating fob database 212 with the security keys for facilitating authentication of the unique RFID reader 104 identifier. In addition, personalization system 116 may populate on database 212 a unique fob 102 identifier for use by RFID reader 104 in determining whether fob 102 is authorized to access system 100. Personalization system 116 may populate (*e.g.*, inject) the encrypted fob 102 account number into fob database 214 for later providing to an authenticated RFID reader 104.

In one exemplary embodiment, personalization system 116 may include any standard computing system as described above. For example, personalization system 116 may include a standard personal computer containing a hardware security module operable using any conventional graphic user interface. Prior to populating the security key information account number and unique identifying information into the fob 102 or RFID reader 104, the hardware security module may authenticate the fob 102 and RFID reader 104 to verify that the components are authorized to receive the secure information.

FIGS. 6A-B illustrate an exemplary flowchart of a personalization procedure which may be used to personalize fob 102 and/or RFID reader 104. Although the following description discusses mainly personalization of fob 102, RFID reader 104 may be personalized using a similar process. The personalization process, which occurs between the personalization system 116 and the device to be personalized (*e.g.*, fob 102 or RFID reader 104), may begin, for example at step 602. Mutual authentication may occur between the personalization system 116 and the device to be authenticated in much the same manner as was described above with regard to

fob 102 mutually authenticating with RFID reader 104. That is, personalization system 116 may transmit a personalization system 116 identifier to the device to be authenticated which is compared by the device authentication circuitry 210, 308 against personalization system identifiers stored in the device database 212, 310. Where a match does not occur (step 604), the personalization process may be aborted (step 612). Where a match occurs (step 604), the personalization system may prepare a personalization file to be provided to the device to be personalized (step 606). If the personalization system is operated manually, the personalization file may be entered into the personalization system 116 using any suitable system interface such as, for example, a keyboard (step 606). Where the personalization system 116 operator elects to delay the preparation of the personalization files, the system 116 may abort the personalization process (step 610). In this context, the personalization file may include the unique fob 102 or RFID reader 104 identifier, security key for loading into database 212 and 310, and/or security keys for decrypting a fob account number which may be loaded in database 320.

Fob 102 may be personalized by direct connection to the personalization system 116 via RF ISO/IEC 14443 interface 114, or the fob 102 may be personalized using RFID reader 104. Personalization system 116 and RFID reader 104 may engage in mutual authentication and RFID reader 104 may be configured to transmit the fob personalization file to fob 102 via RF. Once the fob 102 is presented to RFID reader 104 (steps 608, 614) for personalization, fob 102 and RFID reader 104 may engage in mutual authentication (step 614). Where the fob 102 is not presented to the RFID reader 104 for personalization, the personalization process may be aborted (step 610).

If the fob 102 is detected, the personalization system 116 may create as a part of the personalization file, a unique identifier for providing to the fob 102 (step 616). The identifier is unique in that one identifier may be given only to a single fob. That is, no other fob may have that same identifier. The fob may then be configured and loaded with that identifier (step 618).

The encrypted fob 102 account number may be populated into fob 102 in the same manner as is described with respect to the fob 102 unique identifier. That is, personalization system 116 may pre-encrypt the account data (step 640) and inject the encrypted account into fob database 214 (step 622). The encrypted account

data may be loaded (*e.g.*, injected) into the fob 102 using RFID reader 104 as discussed above.

Once the personalization file is populated into the fob 102, the populated information is irreversibly locked to prevent alteration, unauthorized reading and/or unauthorized access (step 624). Personalization system 116 may then create a log of the personalization file information for later access and analysis by the personalization system 116 user (step 626).

It should be noted that in the event the personalization process is compromised or interrupted (step 628), the personalization system 116 may send a security alert to the user (step 630) and the personalization process may be aborted (step 612). On the other hand, where no such compromising or interruption exists, the personalization system 116 may be prepared to begin initialization on a second device to be personalized (step 632).

FIGS. 7A-B illustrate another exemplary embodiment of a personalization process which may be used to personalize RFID reader 104. RFID reader 104 may be in communication with a personalization system 116 via RFID reader USB connection 316 (step 702). Once connected, personalization system 116 may establish communications with the RFID reader 104 and RFID reader 104 may provide personalization system 116 any RFID reader 104 identification data presently stored on the RFID reader 104 (step 704). In accordance with step 708, where the RFID reader 104 is being personalized for the first time (step 706) the RFID reader 104 and the personalization system 116 may engage in mutual authentication as described above with respect to FIGS. 6A-B. After the mutual authentication is complete, personalization system 116 may verify that RFID reader 104 is properly manufactured or configured to operate within system 100. The verification may include evaluating the operation of the RFID reader 104 by determining if the RFID reader will accept predetermined default settings. That is, the personalization system 116 may then provide the RFID reader 104 a set of default settings (step 708) and determine if the RFID reader 104 accepts those settings (step 712). If RFID reader 104 does not accept the default settings, personalization system 116 may abort the personalization process (step 714).

If the personalization system 116 determines that the personalization process is not the first personalization process undertaken by the RFID reader 104

(step 706), personalization system 116 and RFID reader 104 may engage in a mutual authentication process using the existing security keys already stored on RFID reader 104 (step 710). If authentication is unsuccessful (step 712), the personalization system 116 may abort the personalization process (step 714).

Where the personalization system 116 and the RFID reader 104 successfully mutually authenticate, the personalization system 116 may update the RFID reader 104 security keys (step 716). Updating the security keys may take place at any time as determined by a system 100 manager. The updating may take place as part of a routine maintenance or merely to install current security key data. The updating may be performed by downloading firmware into RFID reader 104 (step 718). In the event that the personalization system 116 determines in step 706 that the RFID reader 104 is undergoing an initial personalization, the firmware may be loaded into the RFID reader 104 for the first time. In this context, "firmware" may include any file which enables the RFID reader 102 to operate under system 100 guidelines. For example, such guidelines may be directed toward the operation of RFID reader protocol/sequence controller 314.

Personalization system 116 may then determine if the personalization keys (*e.g.*, security keys, decryption keys, RFID identifier) need to be updated or if the RFID reader 104 needs to have an initial installation of the personalization keys (step 720). If so, then personalization system 116 may download the personalization keys as appropriate (step 722).

Personalization system 116 may then check the RFID reader 104 to determine if the fob 102 identifiers and corresponding security keys should be updated or initially loaded (step 724). If no updating is necessary the personalization system 116 may end the personalization procedure (step 732). Contrarily, if the personalization system 116 determines that the fob 102 identifiers and corresponding keys need to be updated or installed, the personalization system 116 may download the information onto RFID reader 104 (step 726). The information (*e.g.*, fob security keys and identifiers) may be downloaded in an encrypted format and the RFID reader 104 may store the information in the RFID reader database 310 as appropriate (step 728). The personalization system 116 may then create or update a status log cataloging for later use and analysis by the

personalization system 116 user (step 730). Upon updating the status log, the personalization process may be terminated (step 732).

It should be noted that, in some instances it may be necessary to repersonalize the RFID reader in similar manner as described above. In that instance, the personalization process described in FIGS. 7A and 7B may be repeated.

FIG. 8 illustrates an exemplary flow diagram for the operation of system 100A. The operation may be understood with reference to FIG. 1A, which depicts the elements of system 100A which may be used in an exemplary transaction. The process is initiated when a customer desires to present a fob 102 for payment (step 802). Upon presentation of the fob 102, the merchant initiates the RF payment procedure via an RFID reader 104 (step 804). In particular, the RFID reader sends out an interrogation signal to scan for the presence of fob 102 (step 806). The RF signal may be provided via the RFID reader antenna 106 or optionally via an external antenna 108. The customer then may present the fob 102 for payment (step 808) and the fob 102 is activated by the RF interrogation signal provided.

The fob 102 and the RFID reader 104 may then engage in mutual authentication (step 810). Where the mutual authentication is unsuccessful, an error message may be provided to the customer via the RFID optical and/or audible indicator (step 814) and the transaction may be aborted (step 816). Where the mutual authentication is successful (step 814), the RFID reader 104 may provide the customer with an appropriate optical and/or audible message (*e.g.*, "transaction processing" or "wait") (step 818). The fob protocol/sequence controller 208 may then retrieve from database 214 an encrypted fob account number and provide the encrypted account number to the RFID reader 104 (step 820).

The RFID reader 104 may then decrypt the account number and convert the account number into magnetic stripe (ISO/IEC 7813) format (step 822) and provide the unencrypted account number to the merchant system 130 (step 828). In particular, the account number may be provided to the POS 110 device for transmission to the merchant network 112 for processing. Exemplary processing methods according to the present invention are discussed with respect to FIGs. 10-13, shown below. Upon processing, the POS device 110 may then send an optical

and/or audible transaction status message to the RFID reader 104 (step 830) for communication to the customer (step 832).

The methods for processing the transactions may include one of several formats as required by the fob issuer. For example, one processing method may include processing the transaction under a preloaded fob format wherein a payment value (*e.g.*, monetary value, reward points value, barter points value, etc.) may be preloaded into an preloaded value account or data file prior to permitting usage of the fob. In this way, the user may be permitted to set aside a payment amount for transactions for goods and services using the fob. During processing of the transaction, approval of the transaction may involve comparing the transaction amount to the amount stored (or remaining) in the preloaded value data file. Comparison may be made by a preloaded value processing system wherein the preloaded value processing system may compare the transaction amount to be processed to the preload value data file. Where the transaction amount exceeds the amount stored in the preloaded value account, the preloaded value processing system may deny authorization for completion of the transaction. Contrarily, where the transaction amount does not exceed the amount stored in the preloaded value data file account the preloaded value processing system may provide for authorization of the transaction.

An exemplary preloaded value processing system 1000 is shown with respect to FIG. 10. Preloaded value processing system 1000 may include a fob 102 including a transponder 114, which is in communication with a merchant system 130 via a RFID reader 104 or a computer interface 134 as is described with respect to FIG. 1A. The merchant system may be in communication with an issuer system 1010, where the issuer system 1010 may be maintained by any entity (*e.g.*, financial institution, American Express®, Visa® and/or MasterCard®, etc.) which permits the fob 102 user to store a preload value amount in a preloaded value account (e.g., data file) maintained on an issuer database 1012 of similar construction as database 212. The issuer system 1000 may further include one or more process servers for processing a fob transaction. As shown, a POS device 110 (included in merchant system 130) may be in communication with an issuer account server (IAS) 1014 for receiving the fob account information from POS device 110. IAS 1014 may be in further communication with a preloaded value authorization server

(PLAS) 1016 for processing transactions involving a preloaded value fob. The PLAS 1016 may be in further communication with an issuer database 1012 for retrieving funds from the preloaded value data file (not shown) which are necessary for satisfying the preloaded fob or merchant transaction request.

As used herein, the term "issuer" or "account provider" may refer to any entity facilitating payment of a transaction using a fob, and which included systems permitting payment using at least one of a preloaded and non-preloaded fob. Typical issuers maybe American Express®, MasterCard®, Visa, Discover®, and the like. In the preloaded value processing context, an exchange value (*e.g.*, money, rewards points, barter points, etc.) may be stored in a preloaded value data file for use in completing a requested transaction. The exchange value may not be stored on the fob itself. Further, the preloaded value data file may be debited the amount of the transaction requiring the preloaded value account to be replenished. As described more fully below, the preloaded value system platform may be used to complete "direct link" transactions. In which case, the preloaded value account may function as a place holder, perpetually storing a zero value.

The preloaded value data file may be any conventional data file configuration for storing a value (*e.g.*, monetary, rewards points, barter points, etc.) which may be exchanged for goods or services. In that regard, the preloaded value data file may have any configuration as determined by the issuer system 1010.

In exemplary operation, a fob identifying information (*e.g.*, account number or fob marker) may be provided to the POS device 110 in similar manner as was discussed with respect to FIG. 1A. That is, the fob 102 may be presented to the merchant system 130 via a RFID reader 104 or a computer interface 134, which may provide the fob identifying information in Track 1 or Track 2 format. A POS device 110 included in the merchant system 130 may receive the fob 102 identifying information and provide the fob 102 identifying information along with the transaction identifying information (*e.g.*, amount, quantity, merchant identification, etc.) to the issuer system 1010 for authorization. The merchant system 130 may additionally include a merchant system marker or identifier for indicating a merchant system identity. The merchant system 130 may combine the fob 102 identifying information, the merchant identifying information, or the transaction identifying

information, or any combination thereof, into a merchant transaction request for providing to the issuer system 1010.

The IAS 1014 may receive the transaction and fob identifying information (or merchant transaction request) and recognize that the transaction is being requested relative to a preloaded value account associated with a preloaded fob. That is, the IAS 1014 may recognize that the user has presented a preloaded fob 102 for payment. Recognition of the fob 102 as a preloaded fob may mean that the fob identifying information includes a marker or identifier indicating that the fob is associated with a preloaded value data file. Upon recognition of the marker, the IAS 1014 may forward transaction and fob identifying information to the PLAS 1016 for processing. PLAS 1016 may compare the transaction amount to the value stored or remaining in the preloaded value to determine if authorization should be granted or denied. Where the transaction amount exceeds the value stored in the preloaded value data file the PLAS 1016 may forward a transaction denied message to the IAS 1014 for providing to the merchant system 130. Alternatively, where the transaction amount is less than or equal to the value stored in the preload value data file the PLAS 1016 may deduct from the preloaded value data file the necessary amount for satisfaction of the transaction.

As noted above, in one exemplary embodiment of the present invention, the PLAS 1016 may provide a transaction denied message to the IAS 1014 where the amount stored in the preloaded value account is less than required for satisfying the merchant or fob transaction request. In this instance, where the preloaded value falls below a predetermined minimum level (*e.g.*, minimum depletion level), it may be necessary for the fob user to reload the preloaded value data file. Reloading of the preloaded value account may take place manually (*e.g.*, by the fob user telephonically or online) or may take place automatically when the value stored in the preloaded value data file is depleted to a predefined level. Where the reloading is done automatically, reloading may occur under rules established by the fob issuer or owner. For example, reloading may occur at preselected time intervals, when the value stored is below a predetermined amount, until a maximum number of reloads in a predetermined time period has occurred or until a maximum reload amount is reached in a predetermined time period.

FIGs. 11A and 11B depict exemplary preloading and reloading processes which may be performed in accordance with the present invention. The preloading and reloading processes may be preformed using one or more servers (*e.g.*, PLAS 1016) in communication with a funding source 1104. Although the processes are demonstrated using a PLAS 1016, it is contemplated that any server for establishing and managing data files may be used. However, to facilitate further understanding of the invention, the preloading and reloading aspects of the invention are described with reference to PLAS 1016.

PLAS 1016 may be used to establish on the server or on a database (e.g., database 1012) a preloaded value account (*e.g.*, data file) (1106). The preload value account may be funded or maintained by a fob issuer which may establish a credit, charge, debit, rewards value account, etc. in connection with a charge or credit card (*e.g.*, Visa, MasterCard, American Express, Discover, etc.), debit or direct debit authorization (DDA) system.

The preloaded value account may be established to at least a predetermined minimum preload amount or value (*e.g.*, minimum preload level) as determined by the account provider and/or the fob user or owner. In this context, the predetermined minimum value (*e.g.*, minimum preload value) required to establish the preloaded value account may vary with respect to a particular fob user. The preloaded value account may be loaded (e.g., preloaded or reloaded) from funds received from one of a funding source account 1104 (American Express, Visa, MasterCard, Discover, etc.). That is, the PLAS 1016 may communicate with the funding source 1104 to obtain funds or value for loading or reloading the preloaded value account (1108).

FIG. 11B shows and exemplary reloading process in accordance with the invention. During operation, a consumer may present to a merchant system 130 the prepaid fob 102 for purchasing goods or services (1110). The preloaded value account is then depleted the value amount paid to the merchant system 130. The process for purchasing goods may be repeated until the value stored in the preloaded value account equals or is less than a minimum level balance (*e.g.*, minimum depletion level). The minimum depletion level may be predetermined by the fob user or fob issuer, and may be the minimum value permitted to be stored in the preloaded value account before the file is to be reloaded.

Once the preloaded value data is depleted such that the minimum depletion level is reached, the PLAS 1016 may trigger an automatic reload to reload the preloaded value account from funds retrieved from the funding source 1104 (1112). The amount of funds retrieved may be sufficient for loading the preloaded value account to the minimum amount described above or to some other predetermined reload value. In one exemplary embodiment, the PLAS 1016 may trigger automatic reloading where a predetermined minimum depletion level (e.g., "minimum level balance") is reached. That is, the preloaded value account may not be entirely depleted to zero value before automatic reloading occurs. In this instance, the PLAS 1016 may charge the funding necessary for automatic reloading against the available funds at funding source 1104. In another exemplary embodiment the automatic reloading may occur where the transaction exceeds the amount stored in or remaining in the preloaded value account. In this way, the preloaded value account may be restored to an amount necessary for completion of the transaction. For example, where automatic reloading restores the preloaded value account to a value suitable for transaction completion, the preloaded value account may be automatically reloaded prior to processing the transaction.

In another exemplary embodiment, automatic reloading may occur based on different user or issuer automatic reload criteria. Other automatic reload criteria may include, but are not limited to, reloading until a defined maximum load amount in a defined time period is reached, reloading at a selected periodic reoccurring time interval (*e.g.*, once a month), reloading as permitted until a defined maximum number of reloads in a specified time period is reached, or reloading until a defined maximum reload amount is reached in a specified time period, etc. In some instances, reloading may be done manually, such as, for example, when the fob user contacts the issuer (or any other entity or system which may facilitate the request) to provide a specified funding source for use in reloading the preloaded account and specifies the amount to be preloaded.

In one particular embodiment, the PLAS 1016 may determine whether a full or partial reload may be performed based on the class of transactions requested or the merchant requesting the transaction. The PLAS 1016 may identify a merchant or transaction as a desired merchant or transaction for triggering an automatic reload based on a merchant or transaction identifier or marker. The PLAS 1016

may then reload the account in accordance with any automatic reload criteria defined by the fob user, fob issuer and/or any other entity or system.

Where the fob user initiates the transaction using a computer interface 134, the PLAS 1016 may notify the fob user that an automatic reload has been performed due to the merchant or transaction preferred status. The PLAS 1016 may issue the notification via the IAS server, which, in turn, may send the notification to a fob user registered email account or other means for notifying the fob user (e.g., pager, cell phone, personal digital assistant and/or the like). The email account may be accessible by the fob user via any on-line global network.

In some instances where the transaction is initiated via a computer interface 134, the fob user may be notified that a manual reload is required to complete a transaction. The issuer system 1010 may provide the notification via a server (e.g., IAS 1014 or PLAS 1016) in communication with a computer interface 134. The notification may be provided in real-time, wherein the notification is sent to an e-mail account accessible to the fob user. The system may then enable the fob user to access to issuer database 1012 to identify an amount or funding source 1014 for completing the transactions. Further still, the fob user may be permitted to contact the issuer telephonically to manually reload the preloaded data file. Alternatively, the fob user may be permitted to contact the issuer virtual authorizing agent in real-time for specifying reload requirements. An exemplary method for permitting real-time communications between fob user (e.g., account holder) and an issuer virtual agent is described in commonly assigned U.S. Patent Application No. 10/155,360, SYSTEM AND METHOD FOR INTERACTIVE SECURE DIALOG BETWEEN CARDHOLDER AND ISSUER, filed May 23, 2002, herein incorporated by reference.

In another exemplary embodiment, the preloaded value transaction processing system may permit approval of transactions where the transaction value exceeds the preloaded amount stored in the preloaded value data file. That is, the preloaded fob may be used for purchases exceeding the preloaded value amount provided that the charge submitted by the merchant is less than or equal to the maximum reload permitted plus the amount stored on the card at the time the charge is submitted.

In another exemplary embodiment, the preloaded value system may approve transactions based on a particular merchant's transaction processing protocol. Where the issuer has reviewed and/or approved a merchant's transaction processing method, the system may take the method in consideration in determining whether to approve a merchant's transaction request. For example, a merchant's transaction processing method may include the merchant submitting transaction requests which exceed the preloaded value amount, but the actual charge may be less than or equal to the preloaded value amount. In this instance, the preloaded value transaction processing system may still be configured to approve the transaction request. The processing system may recognize that a transaction came from a particular merchant and institute a predetermined approval protocol correlative to that merchant, since the approval protocol may include information that the merchant is sending a transaction request exceeding the actual charge.

The system may use any one of the acceptable techniques for identifying merchants, such as recognition of the merchant ID, or a marker appended to the transaction, etc. The processing system may correlate the merchant ID with a merchant protocol for requesting a transaction approval of an amount greater than the preloaded value (or reload value), and approve the merchant request accordingly.

In accordance with an alternate exemplary embodiment of a preloaded value processing system 1000, upon receiving the transaction request from the IAS 1014, the PLAS 1016 may evaluate the transaction request based upon several risk criteria established by the issuer. If all the criteria are successfully met, then the PLAS 1016 may send authorization of the transaction (*e.g.*, "transaction granted") to the IAS 1014 for providing to the merchant system 130. Simultaneous with, subsequent to, providing the transaction authorization to the IAS 1014, the PLAS 1016 may seek satisfaction of the transaction from the fob account maintained on the account provider database 1012. The transaction request may be provided to the IAS 1014 for processing. That is, the IAS 1014 may seek to deduct the transaction value from the balance of the amount stored in the preloaded value data file.

FIG. 12 depicts an exemplary embodiment of another transaction processing system ("direct link" system) 1200 in accordance with the present. More particular, FIG. 12 depicts a direct link system 1200 which may be used to process transaction request. In this context, a direct link system may be any system which facilitates satisfaction of a transaction using a fob directly linked to an account which stores an exchange value (*e.g.*, money, credit or charge, or rewards points, etc.). In this instance, the account is not preloaded. Additionally, the account may be linked to a contact product such as a credit, debit, and/or DDA card, and the like, which may be presented for payment of goods and services. In this regard, the fob (here called "direct link fob") and the card are associated with the same funding source and the user may seek satisfaction of a transaction from the funding source independent of whether the fob or card is used.

In this exemplary direct link system 1200, the fob 102 (not shown) user may not establish a preloaded account. Instead, the fob 102 may be associated with a fob transaction account which may be used to provide payment to the merchant for goods and services.

Direct link system 1200 may have similar elements as described with respect to FIG. 10. Moreover, in accordance with an exemplary embodiment of the invention, a transaction request associated with a direct link fob may be processed using the preloaded value system described above, where the preloaded value data file is used as a place holder storing a zero value. The account established by the issuer for fob use is treated as the funding source for satisfying direct link transactions. As shown, the system 1200 may include a fob 102 (not shown) including a transponder 114, which is in communication with a merchant system 130 via a RFID reader 104 (not shown) or a computer interface 134 (not shown) as is described with respect to FIG. 1A. The merchant system 130 may be in communication with an account provider system 1010. The issuer system 1010 may include one or more process servers for processing a fob transaction request.

As shown, the POS device 110 may be in communication with a issuer account server (IAS) 1014 for receiving the fob and transaction identifying information from POS device 110. IAS 1014 may be in further communication with a PLAS 1016 for processing transactions including a direct link fob. The PLAS 1016 may be in further communication with a second IAS 1202, although a second

IAS 1202 may not be required where one or more of the existing servers 1014 or 1016 may perform the functions of IAS 1202 described below. However, the IAS 1202 is included herein to simplify the understanding the operation of this exemplary embodiment.

In exemplary operation of system 1200, the fob identifying information (*e.g.*, account number) may be provided to the POS device 110 in similar manner as was discussed with respect to FIG. 1A. That is, the fob 102 may be presented to the merchant system 130 via a RFID reader 104 or a computer interface 134, which may provide the fob identifying information in Track 1 or Track 2 format. A POS device 110 included in the merchant system 130 may receive the fob 102 identifying information and provide the fob 102 identifying information along with the transaction identifying information (*e.g.*, amount, quantity, merchant identification, etc.) to the account provider system 1010 for authorization.

The IAS 1014 may receive the transaction and fob identifying information and recognize that the transaction as being requested relative to a direct link fob associated with an any suitable account for payment (not a stored value account). Recognition of the fob 102 in this instance may mean that the direct link fob identifying information includes a marker or identifier indicating that the fob is associated with the suitable payment account as described above. Upon recognition of the marker, the IAS 1014 may forward transaction and fob identifying information to PLAS server 1016 for processing.

In similar manner as was described with respect to the operation of the preloaded value system of FIG 10, the PLAS 1016 may evaluate the transaction request based upon several risk criteria established by the issuer. Exemplary risk criteria may include, but are not limited to, consideration of amount limits for a specified time period, count limits for a specified time periods, current reserve funding, pre-determined re-funding rules, user, self-defined limits, etc. If all the criteria are successfully met, then the PLAS 1016 may send authorization of the transaction (*e.g.*, "transaction granted") to the IAS 1014 for providing to the merchant system 130.

After providing the transaction authorization to the IAS 1014, the PLAS 1016 may seek authorization of the transaction against the direct link fob account maintained on the issuer database 1012. The authorization request may be

provided to the IAS 1202 for approval. For example, where the direct link account is a charge or credit account the PLAS 1016 may request authorization from the second IAS 1202 and the IAS 1202 may assess the transaction amount against the fob direct link account. That is, the IAS 1202 may seek to record the amount of the transaction in the fob account for payment at the end of the billing cycle (*e.g.*, charge account), or the amount may be recorded on the fob account for payment at a date later than the end of the billing cycle (*e.g.*, credit account).

In the exemplary embodiment described with respect to FIG. 12, the preloaded value data file may be used as a place holder. In that regard, the data file may maintain a zero value, and the data file value is not used to evaluate whether the transaction is to be approved.

In yet another exemplary transaction processing system 1300 depicted in FIG. 13, the merchant system 130 may provide a batch file containing multiple fob transaction requests to be processed. The system 1300 may include a process server 1302 which distinguished between preloaded value and direct link transaction request. That is, process server 1202 may be used for separating the fob transactions which are associated with a preloaded fob account and those that are not associated with a preloaded fob account, as discussed more fully below. The process server 1302 may further be in communication with an IAS 1014 for seeking settlement of the transaction.

In exemplary operation of system 1300, the merchant system 130 may provide the batch file to the process server 1302. The process server 1302 may receive the settlement file and create sub-files of transaction requests relative to the type of fob used in the transaction (*e.g.*, preloaded fob, and direct link fob associated with a charge or credit account). For example, the process server 1302 may create a first fob transaction file (File A) for merchant payables and a second file to be forwarded to the IAS 1204 for processing. Where the sub-file includes merchant payable, the process server 1302 may provide funds to the merchant for payment of the transaction, where the funds provided may be equivalent to the transaction amount minus discount revenues. The funds may be retrieved from the funding source for proving to the merchant.

Alternatively, the process server 1302 may create a second sub-file (File B) for accounts receivable payments and the File B may be forwarded to the IAS 1014.

IAS 1014 may then process the transaction request according to the processes described in FIGs 10 and 12. That is, the IAS 1014 may distinguish the preloaded fob transaction requests from those associated with the direct link fob and process the transactions accordingly.

As can be seen by the above description the transaction processing systems described may distinguish when a fob is used, or when a fob is reloaded. In that regard, the present system may be used to reward points for fob usage and reloading. The points (*e.g.*, loyalty points) may be stored in a points data file maintained on the issuer database (*e.g.*, database 1012). The rewards points may then later be redeemed for exchange for goods and services as desired by the fob user.

In one instance, points may be provided when the fob is used. For example, the IAS 1014 may recognize the that a fob is being used and award points (*e.g.*, loyalty points) to a points data file assigned to the fob user. The loyalty points may be awarded based on any criteria as determined by the fob issuer. Exemplary rewarding criteria may include rewarding points for, for example, frequency of fob usage, amount of individual purchase using the fob, or the total amount of purchases in a given time period.

Where the fob is associated with a preloaded value data file such as that described with respect to FIG. 10, points may be awarded for data file reloading. That is, IAS 1014 may place award points in the points data file relative to the amount loaded or reloaded as required.

It should be noted that the transaction account associated with the fob 102 may include a usage restriction, such as, for example, a per purchase spending limit, a time of day use, a day of week use, certain merchant use and/or the like, wherein an additional verification is required when using the fob outside of the restriction. The restrictions may be personally assigned by the fob 102 user, or the account provider. For example, in one exemplary embodiment, the account may be established such that purchases above $X (*i.e.*, the spending limit) must be verified by the customer. Such verification may be provided using a suitable personal identification number (PIN) which may be recognized by the RFID reader 104 or a payment authorization center (not shown) as being unique to the fob 102 holder (*e.g.*, customer) and the correlative fob 102 transaction account number. Where the

requested purchase is above the established per purchase spending limit, the customer may be required to provide, for example, a PIN, biometric sample and/or similar secondary verification to complete the transaction.

Where a verification PIN is used as secondary verification the verification PIN may be checked for accuracy against a corroborating PIN which correlates to the fob 102 transaction account number. The corroborating PIN may be stored locally (*e.g.*, on the fob 102, or on the RFID reader 104) or may be stored on a database (not shown) at the payment authorization center. The payment authorization center database may be any database maintained and operated by the fob 102 transaction account provider.

The verification PIN may be provided to the POS device 110 using a conventional merchant (*e.g.*, POS) PIN key pad 118 in communication with the POS device 110 as shown in FIG. 1, or a RFID keypad in communication with the RFID reader 104. PIN keypad may be in communication with the POS device 110 (or alternatively, RFID reader 104) using any conventional data link described above. Upon receiving the verification PIN, the RFID reader 104 may seek to match the PIN to the corroborating PIN stored on the RFID reader 104 at database 310 or 320. Alternatively, the verification PIN may be provided to a payment authorization center to determine whether the PIN matches the PIN stored on the payment authorization center database which correlates to the fob 102 account. If a match is made, the purchase may no longer be restricted, and the transaction may be allowed to be completed.

In an alternate embodiment, verification of purchases exceeding the established spending limit may involve biometrics circuitry included in fob 102. FIG. 9 is a schematic block diagram of an exemplary fob 102 wherein fob 102 includes a biometric security system 902. Biometric security system 902 may include a biometric sensor 904 for sensing the fingerprint of the fob 102 user. The biometric sensor 902 may be in communication with a sensor interface/driver 906 for receiving the sensor fingerprint and activating the operation of fob 102. In communication with the biometric sensor 904 and sensor interface 906 may be a battery 903 for providing the necessary power for operation of the biometric security system components.

In one exemplary application of the fob 102 including the biometric security system 902, the customer may place his finger on the biometric sensor to initiate the mutual authentication process between the fob 102 and the RFID reader 104, or to provide secondary verification of the user's identity. The sensor fingerprint may be digitized and compared against a digitized fingerprint stored in a database (*e.g.*, security database 212) included on fob 102. Such comparison step may be controlled by protocol/sequence controller 208 and may be validated by authentication circuit 210. Where such verification is made, the mutual authentication between fob 102 and RFID reader 104 may begin, and the transaction may proceed accordingly. Alternatively, the comparison may be made with a digitized fingerprint stored on a database maintained by the fob 102 transaction account provider system (not shown). The digitized fingerprint may be verified in much the same way as is described above with respect to the PIN.

In one exemplary application of the fob 102 including the biometric security system 902, the system 902 may be used to authorize a purchase exceeding the established per purchase spending limit. In this case, where the customer's intended purchase exceeds the spending limit, the customer may be asked to provide assurance that the purchase is authorized. Accordingly, the customer may provide such verification by placing his finger over the biometric sensor 904. The biometric sensor 904 may then digitize the fingerprint and provide the digitized fingerprint for verification as described above. Once verified, fob 102 may provide a transaction authorized signal to RF transponder 202 (or alternatively to transponder 220) for forwarding to RFID reader 104. RFID reader 104 may then provide the transaction authorized signal to the POS device 110 in similar manner as is done with convention PIN driven systems and the POS device 110 may process the transaction under the merchant's business as usual standard.

In accordance with another exemplary embodiment of the invention, the fob user is provided limited access to a user data file for managing the fob usage and fob user information. The fob user may access the user data file to change, for example, demographic information (*e.g.*, fob user address, phone number, email address, etc.), the funding source (*e.g.*, credit account, charge account, rewards account, barter account, etc.) associated with the fob, view the transaction history,

etc. In addition, the fob user may be permitted to load or reload the account or alter automatic reload parameters (*e.g.*, amount to reload, period for reloading, etc.).

With reference to FIG. 1, the fob user may connect the fob 102 to a computer interface 134 via a USB interface 132. The fob user may then use the computer interface 134 to access the user data file via a network 136. In particular, the network 136 may be in communication with an issuer system (*e.g.* system 1010 of FIG. 10) and may be provided limited access to an issuer server (*e.g.*, server 1014) for managing the fob. The issuer server may be in communication with an issuer system database (*e.g.*, 1012) which stores the information to be managed relative to the user data file. The changes made to the user data file by the fob user may be made to the user data file in real-time, after a brief delay, or after an extended delay. In one instance, changes may be stored in a batch changes file on the issuer database for later batch processing.

The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. For example, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented. Further, the present invention may be practiced using one or more servers, as necessary. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined by the preceding description, and with respect to the attached claims.

CLAIMS

We claim:

1. A transponder-reader payment system comprising:

a. a transponder system responsive to a Radio Frequency (RF) interrogation signal, said transponder system including a universal serial connector and BUS (USB) connector and a transponder database, said transponder database storing at least a transponder system identifier;

b. a Radio Frequency Identification (RFID) reader in RF communication with said transponder system, said RFID reader providing said interrogation signal transponder system and receiving said transponder identifier;

c. a merchant system including merchant identification and a merchant point of interaction device, said merchant point of interaction device in communication with said RFID reader, wherein said RFID reader provides said transponder system identifier to said merchant point of interaction device, said merchant point of interaction device associating said transponder system identifier to a user transaction request and said merchant identifier forming a merchant transaction request, said merchant point of interaction device providing said merchant transaction request to an issuer system;

d. an issuer system for receiving said merchant transaction request comprising:

i. an issuer system server, said issuer system server in communication with said merchant point of interaction device and a user interface, and

ii. an issuer system database including a preloaded value data file and a reload protocol data file, said preloaded value data file and said reload protocol data file associated with said transponder system identifier, said preload value data file storing a predetermined value for use in satisfying a user transaction request;

e. a first funding source associated with said transponder system identifier and said preloaded value data file, said funding source in communication with said issuer system, said funding source containing a funding source value; and

f. a user interface in communications with said issuer system for use in updating at least one of said preloaded value data files and said reload protocol data file.

2. A transponder-reader payment system according to Claim 1 wherein said predetermined value is preloaded into said preloaded value data file prior to transponder system usage, said predetermined value greater than zero.

3. A transponder-reader payment system according to Claim 2 wherein said issuer system compares said user transaction value to said predetermined value.

4. A transponder-reader payment system according to Claim 3 wherein said user system server retrieving at least a portion of said user transaction value from said preloaded value data file and providing a transaction approved transmission and said portion of said user transaction value to said merchant system.

5. A transponder-reader payment system according to Claim 4 wherein said issuer system server deducts at lest a portion of said user transaction value from said preloaded value data file forming a deplete value data to be of a depleted value, said depleted value less than said preloaded value.

6. A transponder-reader payment system according to Claim 5 wherein said issuer system server retrieves said portion of said funding source value and increments said preloaded value data file said portion of said funding source value.

7. A transponder-reader payment system according to Claim 6 wherein said issuer system server retrieves said portion of said funding source value in accordance with said reload protocol data file, said reload protocol data file including at least one reload indicia.

8. A transponder-reader payment system according to Claim 7, wherein said transponder system identifies and at least one update reload indicia is provided to said user interface said user interface further providing said transponder system identifier and said at least one update reload indicia.

9. A transponder-reader payment system according to Claim 8, wherein issuer system server updates aid at least one reload indicia in accordance with said at least one update reload indicia said at least one update reload indicia corresponding to said at least one reload indicia.

10. A transponder-reader payment system according to Claim 9, wherein said updating said at least one reload indicia is performed in real-time.

11. A transponder-reader payment system according to Claim 9, wherein said at least one reload indicia corresponds to said merchant system identifier.

12. A transponder-reader payment system according to Claim 11, wherein said at least one reload indicia corresponds to a minimum depletion value, said issuer system server incrementing said preloaded value data file where said depleted value is less than or equal to said minimum depletion value.

13. A transponder-reader payment system according to Claim 9, wherein said at least one reload indicia may include a maximum load value.

14. A transponder-reader payment system according to Claim 12, wherein said at least one reload indicia may include incrementing said preloaded value data file in accordance with a predetermined time period.

15. A transponder-reader payment system according to Claim 12, wherein said preloaded value data file is incremented a predetermined number of occurrences.

16. A transponder-reader payment system according to Claim 12, further including a second funding source in communication with said issuer system server, and said preload value data file, said second funding source containing a second funding source value.

17. A transponder-reader payment system according to Claim 16, wherein said issuer system server retrieves at least a portion of said second funding source value and increments said preloaded value data file said at least a portion of said second funding source value.

18. A transponder-reader payment system according to Claim 3, wherein said user transaction value is greater than said predetermined value, said issues system server providing a transaction authorization required notice to said user interface.

19. A transponder-reader payment system according to Claim 18, wherein said transaction authorization required notice is provided in real-time.

20. A transponder-reader payment system according to Claim 19, wherein said transaction authorization required notice is provided to a message retrieval account, wherein a transaction approved transmission is provided to said issuer system server via said user interface.

21. A transponder-reader payment system according to Claim 20, wherein said message retrieval account is accessible via said user interface.

22. A method of Radio Frequency Identification transponder-reader payment comprising:

a. providing a transponder system identifier to a merchant system, associating the transponder system identifier to a merchant system identifier and a user transaction request forming a merchant transaction request, the user transaction request containing a transaction value and a transaction identifying marker;

b. providing the merchant transaction request to an issue system server; and comparing said user transaction request to a preloaded value data file, the preloaded value data file associated with a transponder system identity, the preloaded value data file containing a value.

23. A method according to Claim 22, further comprising:

a. determining that the user transaction is less than or equal to the preloaded data file value;

b. retrieving a portion of the preloaded data file value and providing the portion of the preloaded data file value to the merchant system;

c. deducting the portion of the preloaded data file value from the preloaded data file value forming a depleted preloaded data file value;

d. determining that the depleted preloaded data file value is one of less than and equal to a minimum depletion level;

e. replacing at least a portion of the deducted portion of the preloaded data file value according to a reload protocol.

24. A method according to Claim 23, wherein the replacing is performed in response to the merchant system identifier.

25. A method according to Claim 23, wherein the replacing is performed in response to the transaction identifying marker.

26. A method according to Claim 23, wherein the replacing at least a portion of the depleted portion of the preloaded data file includes retrieving at least a portion of the depleted portion from at least one of a first funding source and a second funding source.

27. A method according to Claim 23, further comprising:

providing the transponder system identifier to an issuer system server via a user interface remote from the issuer system;

providing in real-time an update reload protocol to the issuer system server, the issuer system server updating in real-time the reload protocol in accordance with the provided update reload protocol.

28. A method of providing a Radio Frequency Identification transponder-reader payment system comprising:

a. providing a transponder system identifier and at least one load indicia to an issuer system server in real-time;

b. forming a load criteria protocol including the at least one load indicia; and

c. loading a preloaded data file account with value in accordance with the load indicia.

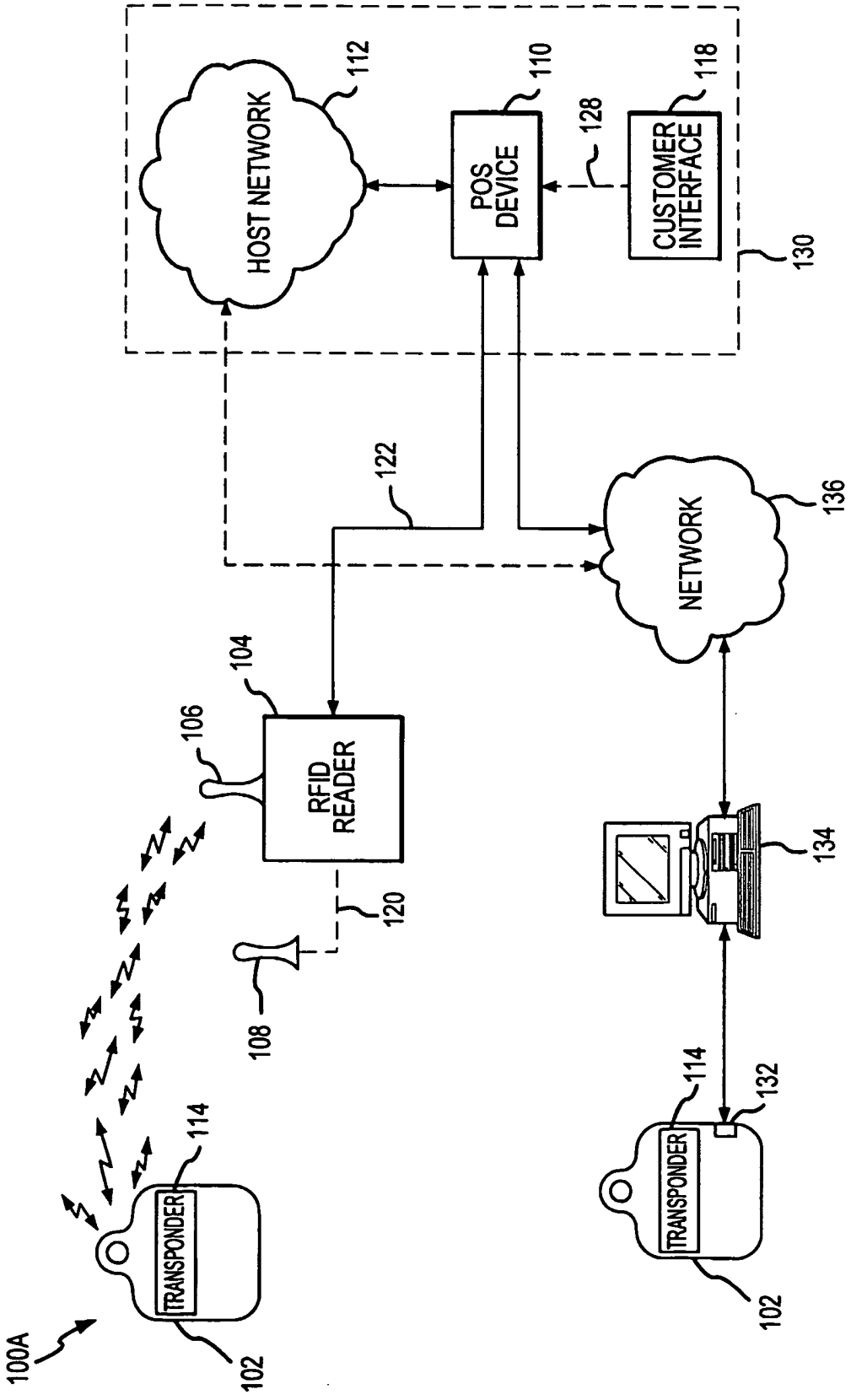

HOST NETWORK
112
POS DEVICE
110
128
CUSTOMER INTERFACE
118
130
122
NETWORK
136
104
RFID READER
106
120
108
134
114
132
TRANSPONDER
TRANSPONDER
114
100A
102
102

FIG.1A

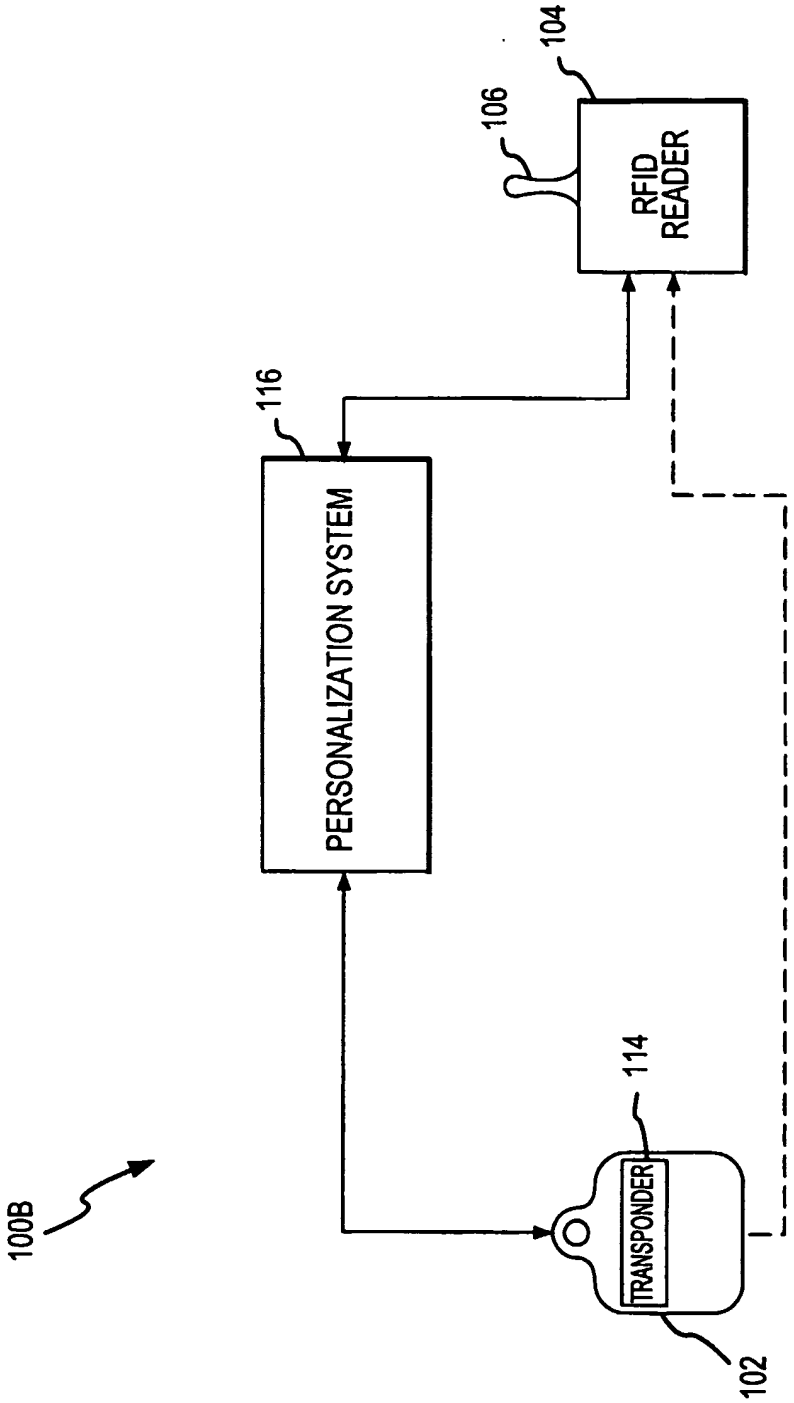

100B
102
TRANSPONDER
114
PERSONALIZATION SYSTEM
116
RFID READER
106
104

FIG.1B

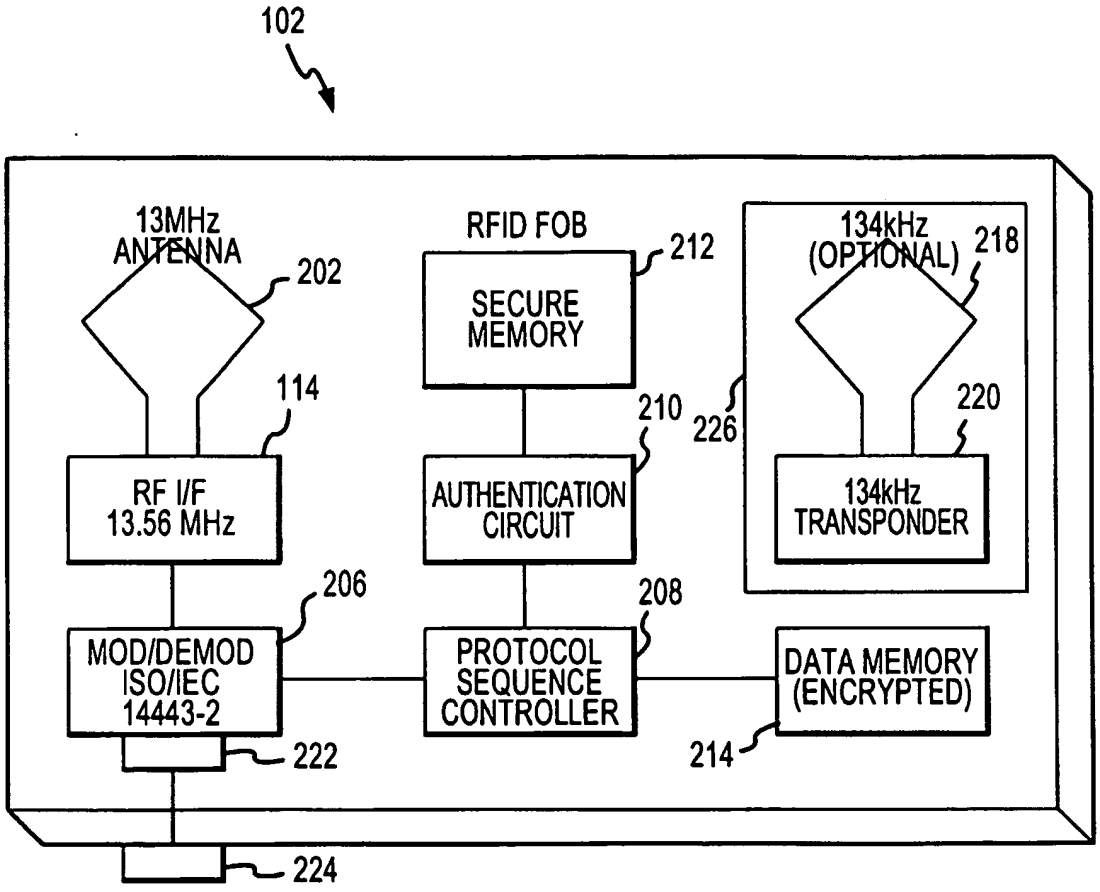

102
13MHz ANTENNA
202
114
RF I/F 13.56 MHz
206
MOD/DEMOD ISO/IEC 14443-2
222
224
RFID FOB
212
SECURE MEMORY
210
AUTHENTICATION CIRCUIT
208
PROTOCOL SEQUENCE CONTROLLER
134kHz (OPTIONAL)
218
226
220
134kHz TRANSPONDER
DATA MEMORY (ENCRYPTED)
214

FIG.2

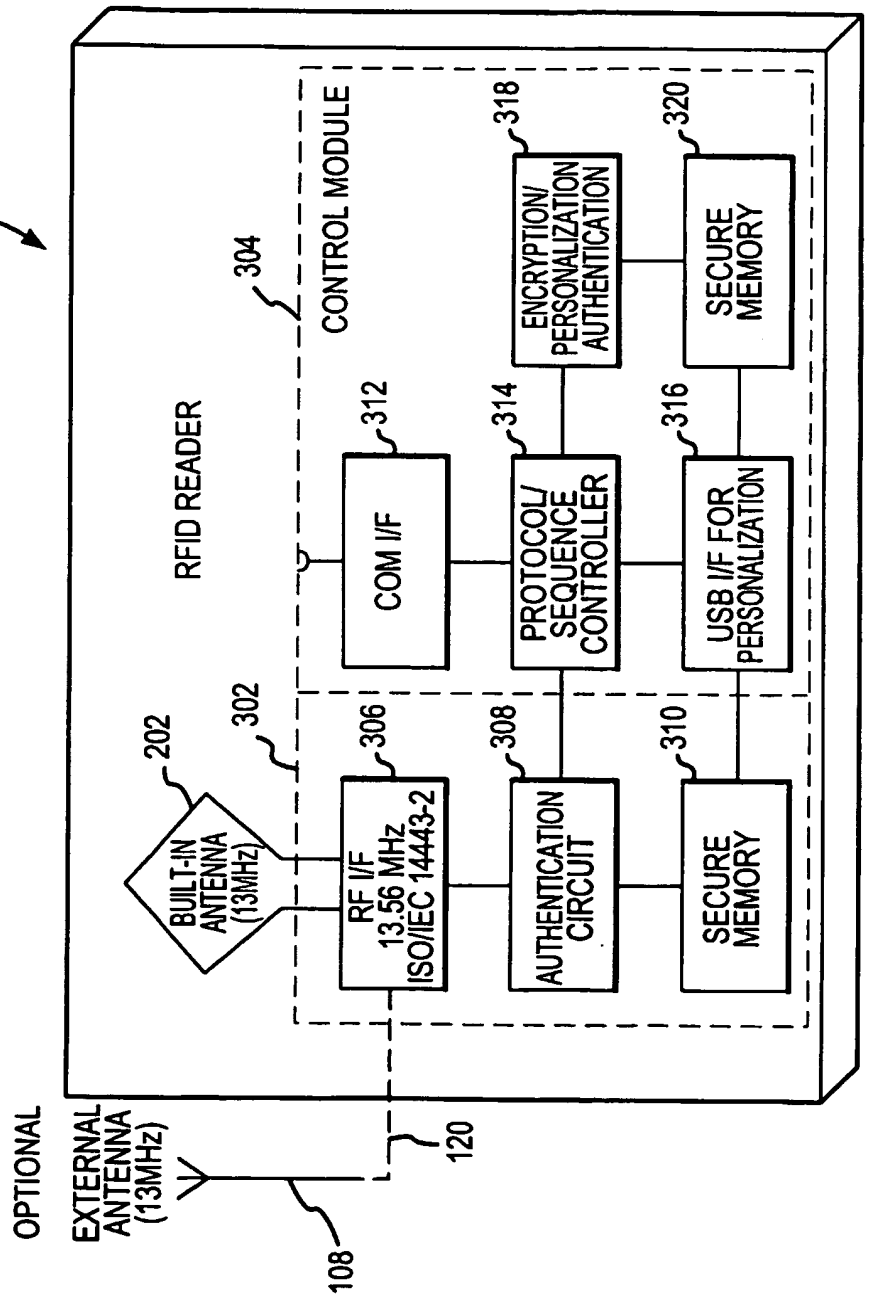

104
RFID READER
CONTROL MODULE
304
302
202
BUILT-IN ANTENNA (13MHz)
306
RF I/F 13.56 MHz ISO/IEC 14443-2
308
AUTHENTICATION CIRCUIT
310
SECURE MEMORY
312
COM I/F
314
PROTOCOL/ SEQUENCE CONTROLLER
316
USB I/F FOR PERSONALIZATION
318
ENCRYPTION/ PERSONALIZATION AUTHENTICATION
320
SECURE MEMORY
120
OPTIONAL
EXTERNAL ANTENNA (13MHz)
108

FIG.3

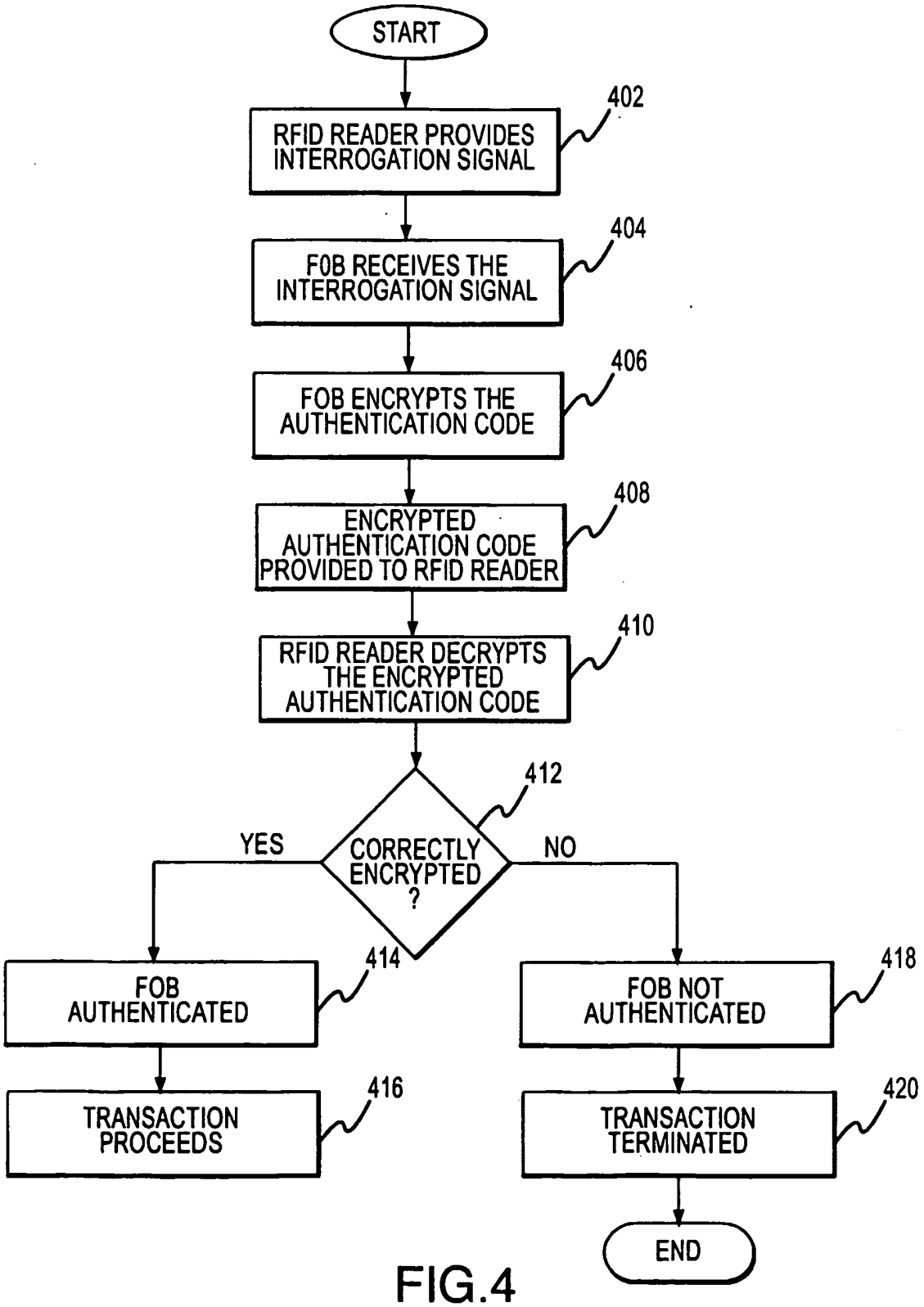

START
RFID READER PROVIDES INTERROGATION SIGNAL
402
F0B RECEIVES THE INTERROGATION SIGNAL
404
FOB ENCRYPTS THE AUTHENTICATION CODE
406
ENCRYPTED AUTHENTICATION CODE PROVIDED TO RFID READER
408
RFID READER DECRYPTS THE ENCRYPTED AUTHENTICATION CODE
410
CORRECTLY ENCRYPTED ?
412
YES
NO
FOB AUTHENTICATED
414
TRANSACTION PROCEEDS
416
FOB NOT AUTHENTICATED
418
TRANSACTION TERMINATED
420
END

FIG.4

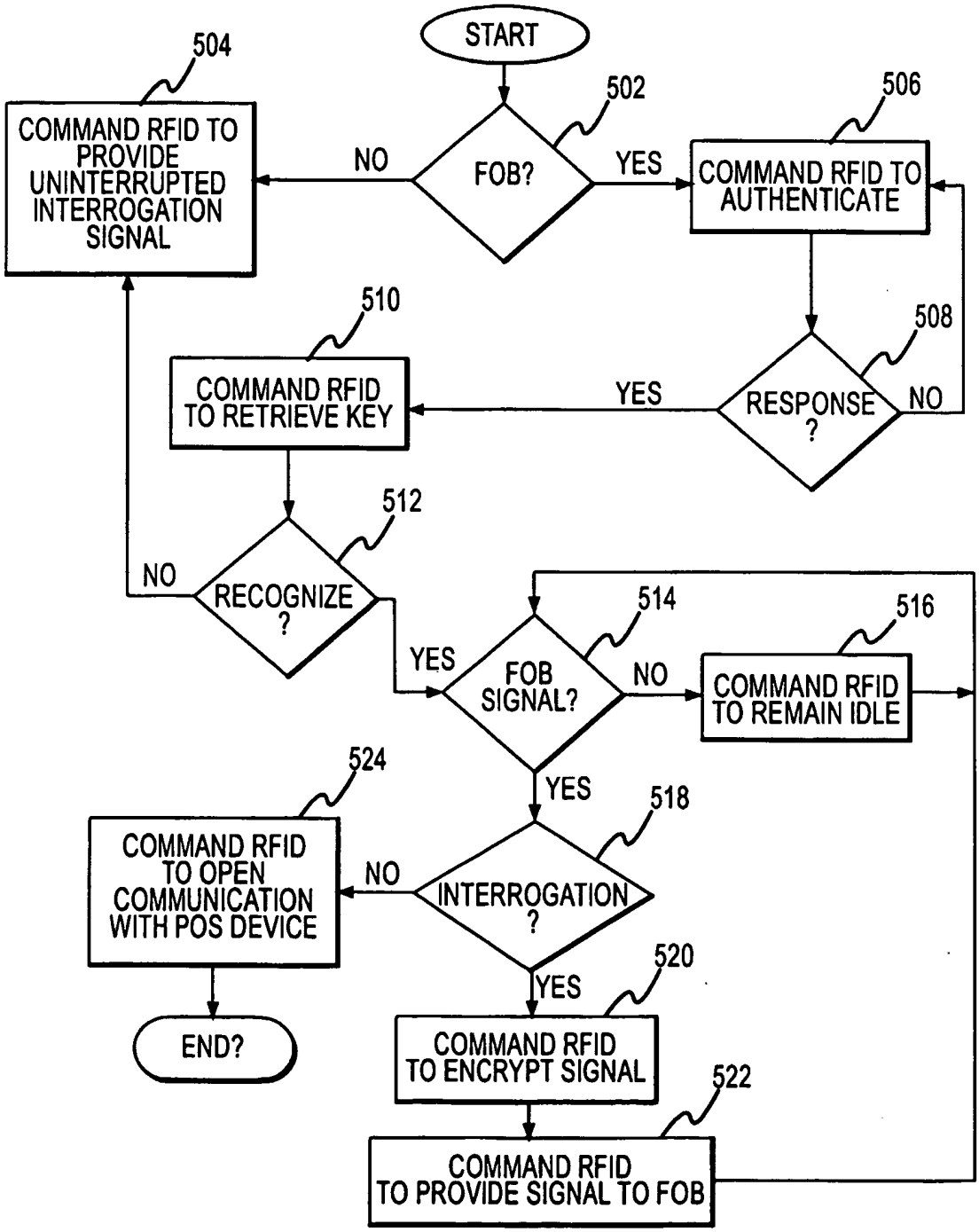

START
502
FOB?
NO
YES
504
COMMAND RFID TO PROVIDE UNINTERRUPTED INTERROGATION SIGNAL
506
COMMAND RFID TO AUTHENTICATE
508
RESPONSE ?
NO
YES
510
COMMAND RFID TO RETRIEVE KEY
512
RECOGNIZE ?
NO
YES
514
FOB SIGNAL?
NO
516
COMMAND RFID TO REMAIN IDLE
YES
518
INTERROGATION ?
NO
524
COMMAND RFID TO OPEN COMMUNICATION WITH POS DEVICE
YES
520
COMMAND RFID TO ENCRYPT SIGNAL
522
COMMAND RFID TO PROVIDE SIGNAL TO FOB
END?

FIG.5

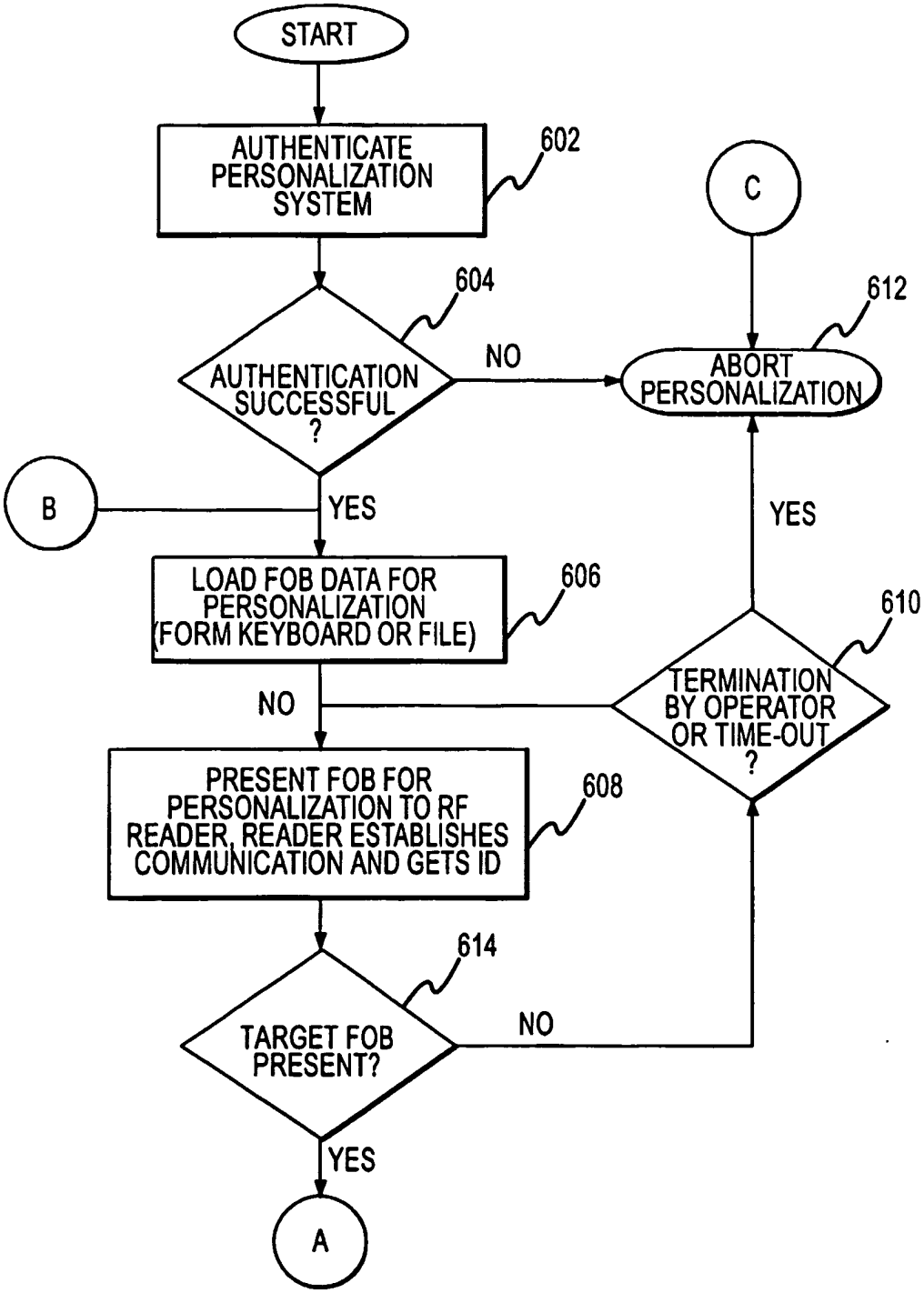

START
AUTHENTICATE PERSONALIZATION SYSTEM
602
C
604
612
AUTHENTICATION SUCCESSFUL ?
NO
ABORT PERSONALIZATION
B
YES
YES
LOAD FOB DATA FOR PERSONALIZATION (FORM KEYBOARD OR FILE)
606
610
TERMINATION BY OPERATOR OR TIME-OUT ?
NO
PRESENT FOB FOR PERSONALIZATION TO RF READER, READER ESTABLISHES COMMUNICATION AND GETS ID
608
614
TARGET FOB PRESENT?
NO
YES
A

FIG.6A

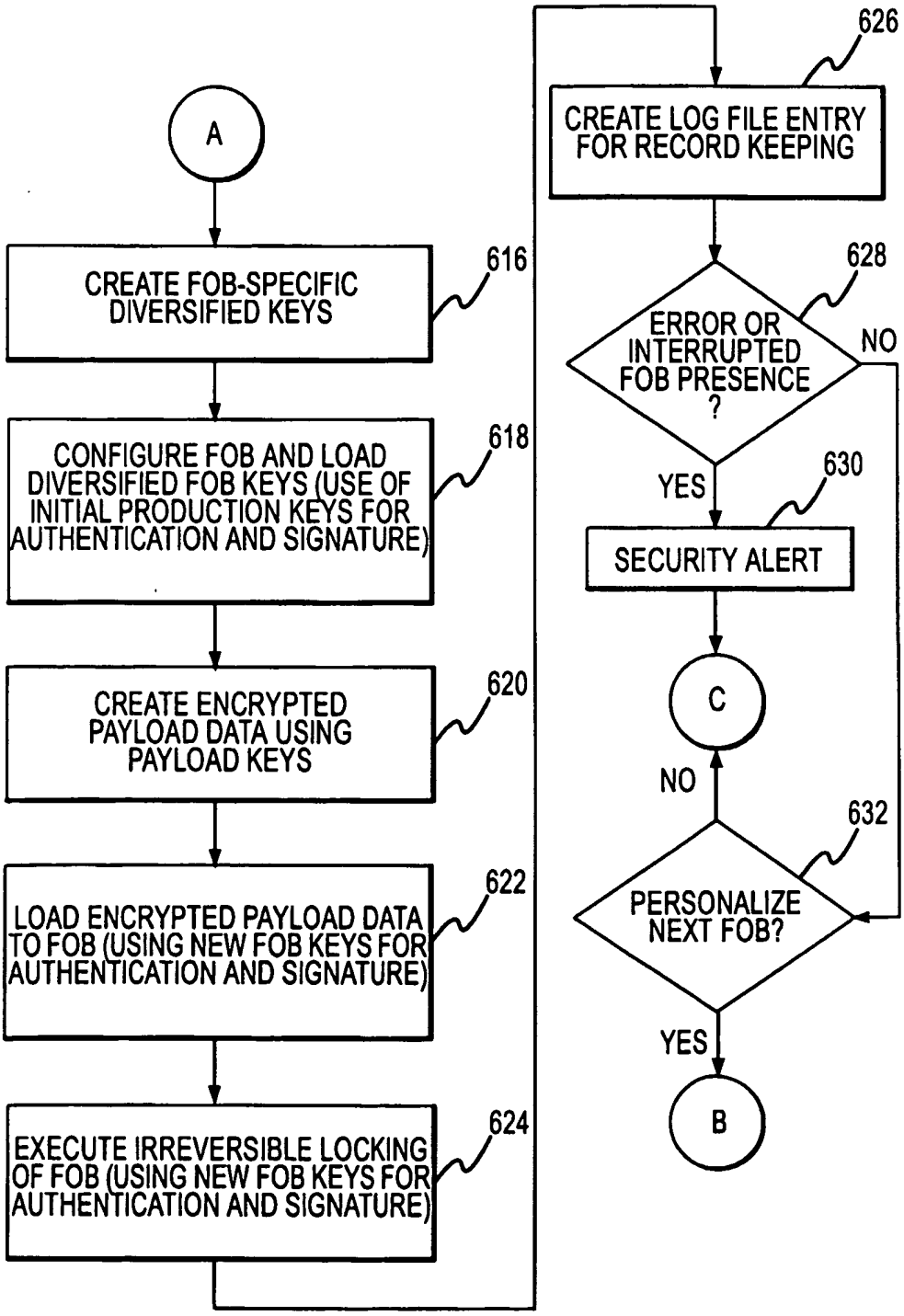

A
CREATE FOB-SPECIFIC DIVERSIFIED KEYS
616
CONFIGURE FOB AND LOAD DIVERSIFIED FOB KEYS (USE OF INITIAL PRODUCTION KEYS FOR AUTHENTICATION AND SIGNATURE)
618
CREATE ENCRYPTED PAYLOAD DATA USING PAYLOAD KEYS
620
LOAD ENCRYPTED PAYLOAD DATA TO FOB (USING NEW FOB KEYS FOR AUTHENTICATION AND SIGNATURE)
622
EXECUTE IRREVERSIBLE LOCKING OF FOB (USING NEW FOB KEYS FOR AUTHENTICATION AND SIGNATURE)
624
626
CREATE LOG FILE ENTRY FOR RECORD KEEPING
628
ERROR OR INTERRUPTED FOB PRESENCE ?
NO
YES
630
SECURITY ALERT
C
NO
632
PERSONALIZE NEXT FOB?
YES
B

FIG.6B

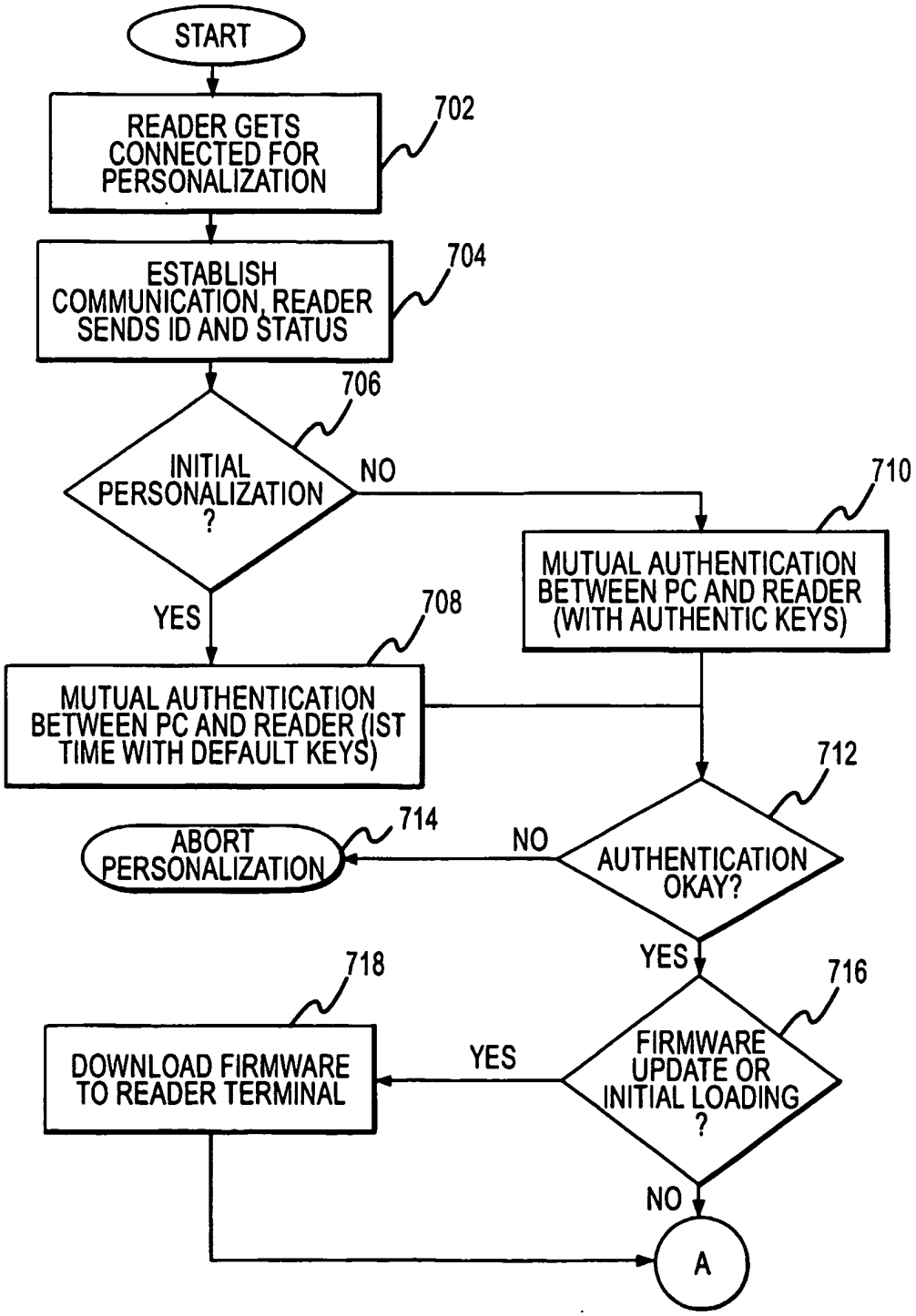

START
READER GETS CONNECTED FOR PERSONALIZATION
702
ESTABLISH COMMUNICATION, READER SENDS ID AND STATUS
704
706
INITIAL PERSONALIZATION ?
NO
710
MUTUAL AUTHENTICATION BETWEEN PC AND READER (WITH AUTHENTIC KEYS)
YES
708
MUTUAL AUTHENTICATION BETWEEN PC AND READER (IST TIME WITH DEFAULT KEYS)
712
ABORT PERSONALIZATION
714
NO
AUTHENTICATION OKAY?
YES
718
716
DOWNLOAD FIRMWARE TO READER TERMINAL
YES
FIRMWARE UPDATE OR INITIAL LOADING ?
NO
A

FIG.7A

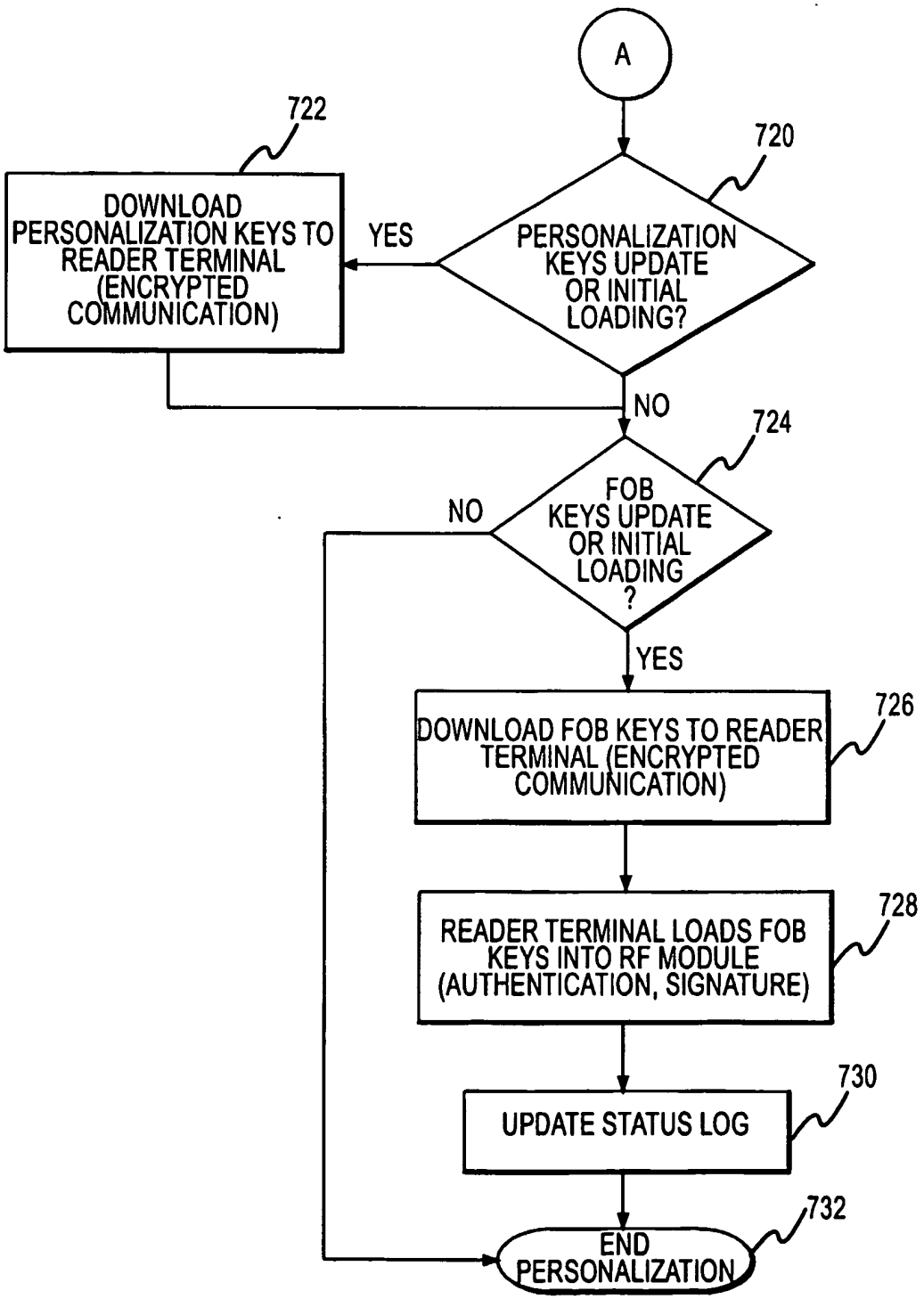

A
720
PERSONALIZATION KEYS UPDATE OR INITIAL LOADING?
YES
722
DOWNLOAD PERSONALIZATION KEYS TO READER TERMINAL (ENCRYPTED COMMUNICATION)
NO
724
FOB KEYS UPDATE OR INITIAL LOADING ?
NO
YES
726
DOWNLOAD FOB KEYS TO READER TERMINAL (ENCRYPTED COMMUNICATION)
728
READER TERMINAL LOADS FOB KEYS INTO RF MODULE (AUTHENTICATION, SIGNATURE)
730
UPDATE STATUS LOG
732
END PERSONALIZATION

FIG.7B

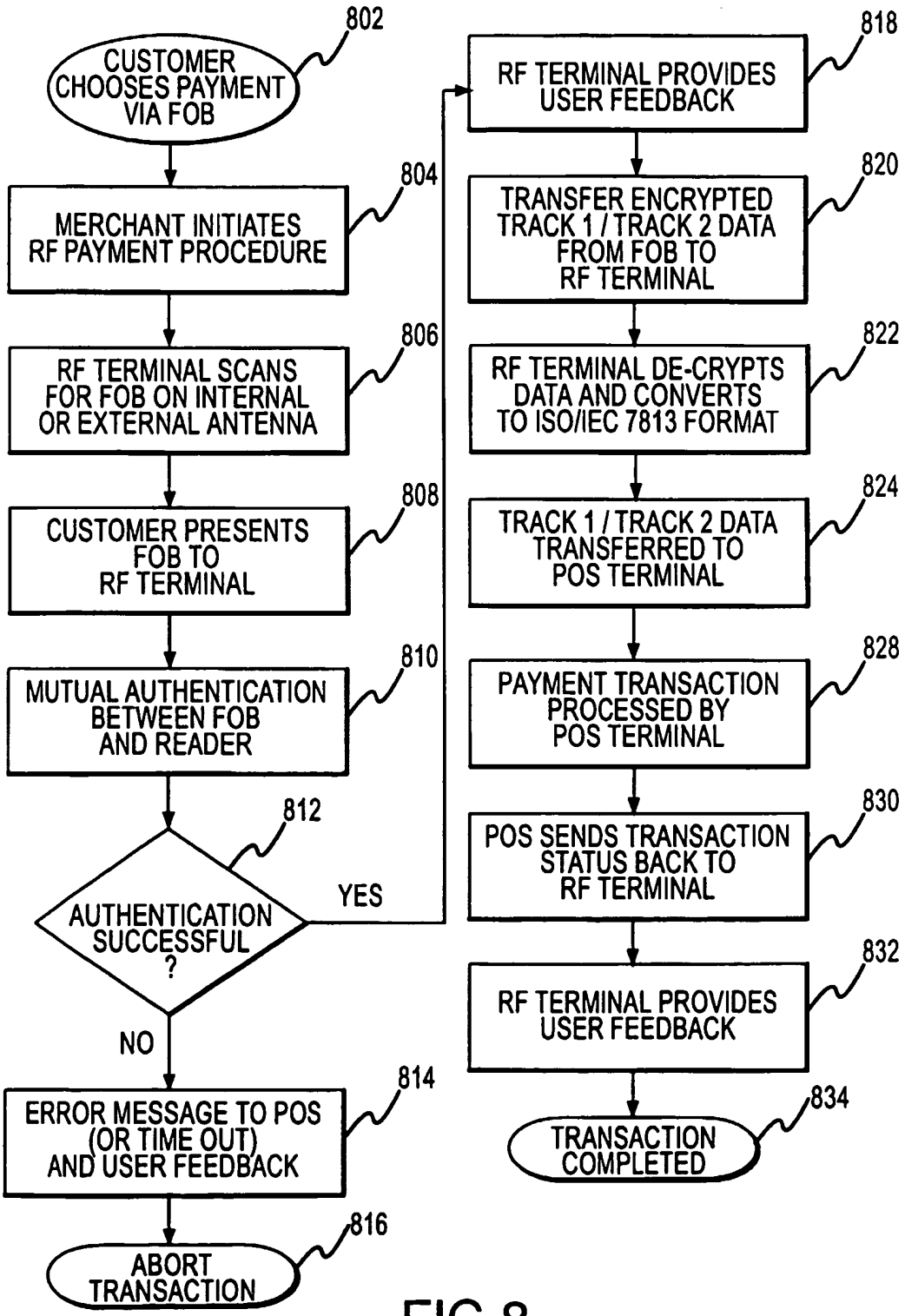

802
CUSTOMER CHOOSES PAYMENT VIA FOB
804
MERCHANT INITIATES RF PAYMENT PROCEDURE
806
RF TERMINAL SCANS FOR FOB ON INTERNAL OR EXTERNAL ANTENNA
808
CUSTOMER PRESENTS FOB TO RF TERMINAL
810
MUTUAL AUTHENTICATION BETWEEN FOB AND READER
812
AUTHENTICATION SUCCESSFUL ?
YES
NO
814
ERROR MESSAGE TO POS (OR TIME OUT) AND USER FEEDBACK
816
ABORT TRANSACTION
818
RF TERMINAL PROVIDES USER FEEDBACK
820
TRANSFER ENCRYPTED TRACK 1 / TRACK 2 DATA FROM FOB TO RF TERMINAL
822
RF TERMINAL DE-CRYPTS DATA AND CONVERTS TO ISO/IEC 7813 FORMAT
824
TRACK 1 / TRACK 2 DATA TRANSFERRED TO POS TERMINAL
828
PAYMENT TRANSACTION PROCESSED BY POS TERMINAL
830
POS SENDS TRANSACTION STATUS BACK TO RF TERMINAL
832
RF TERMINAL PROVIDES USER FEEDBACK
834
TRANSACTION COMPLETED

FIG.8

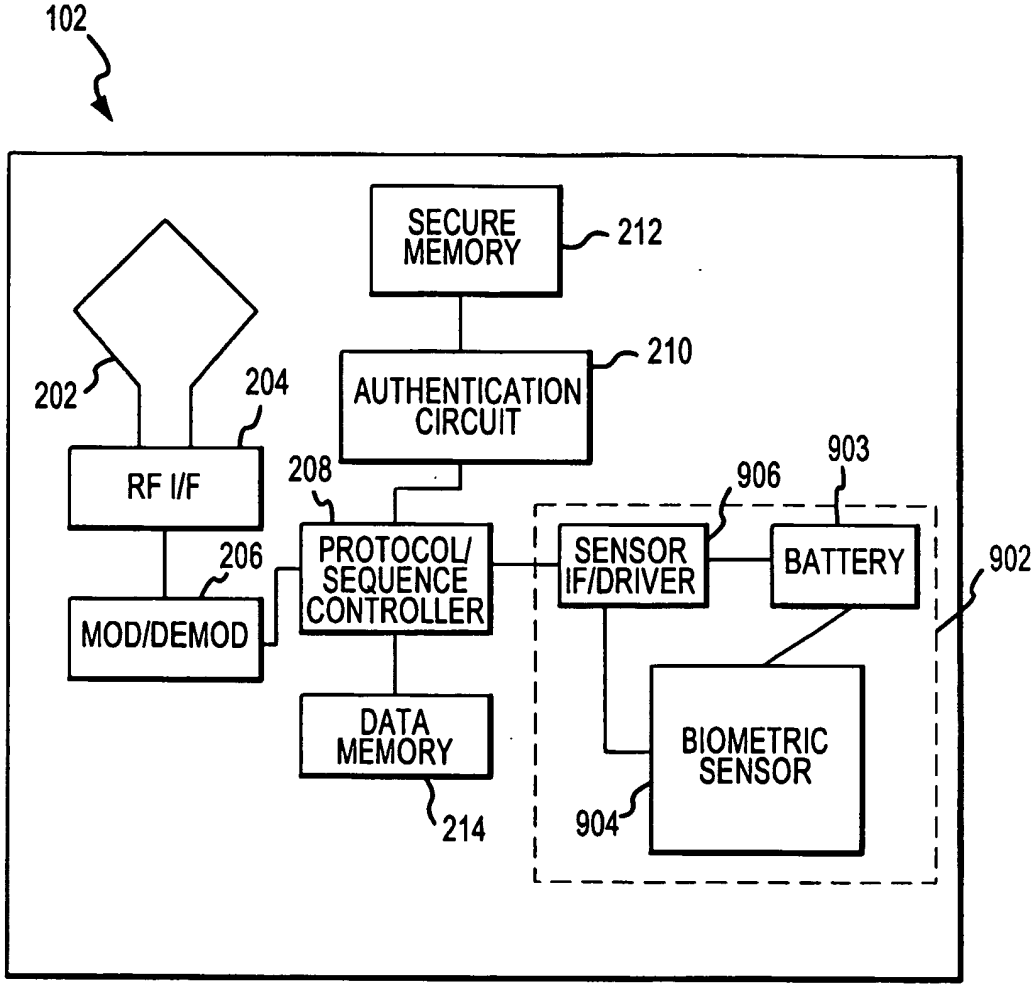

102
SECURE MEMORY
212
AUTHENTICATION CIRCUIT
210
202
204
RF I/F
208
906
903
206
PROTOCOL/ SEQUENCE CONTROLLER
SENSOR IF/DRIVER
BATTERY
902
MOD/DEMOD
DATA MEMORY
214
BIOMETRIC SENSOR
904

FIG.9

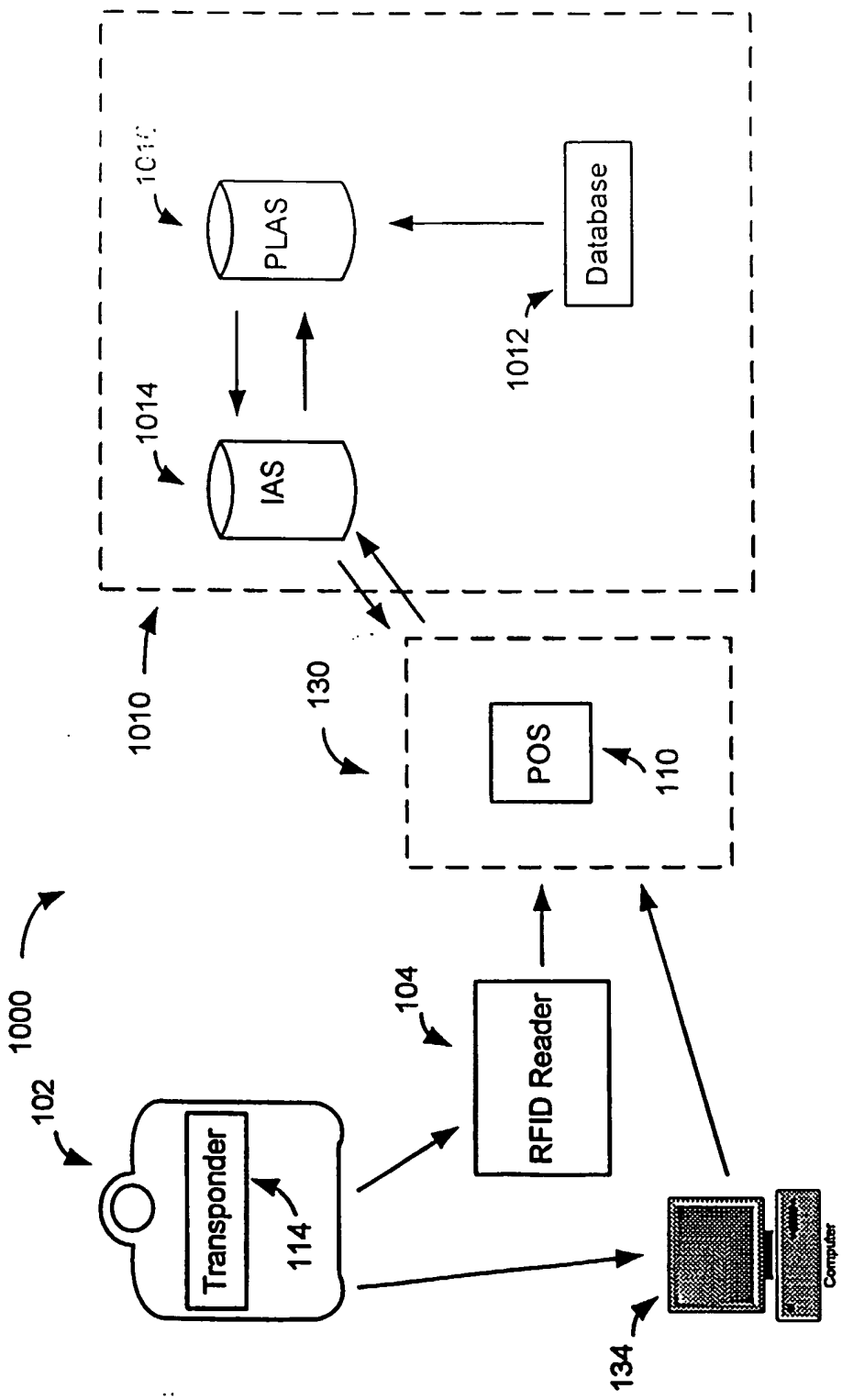

1000
1010
1012
Database
1014
IAS
PLAS
130
POS
110
102
Transponder
114
104
RFID Reader
134
Computer

FIG. 10

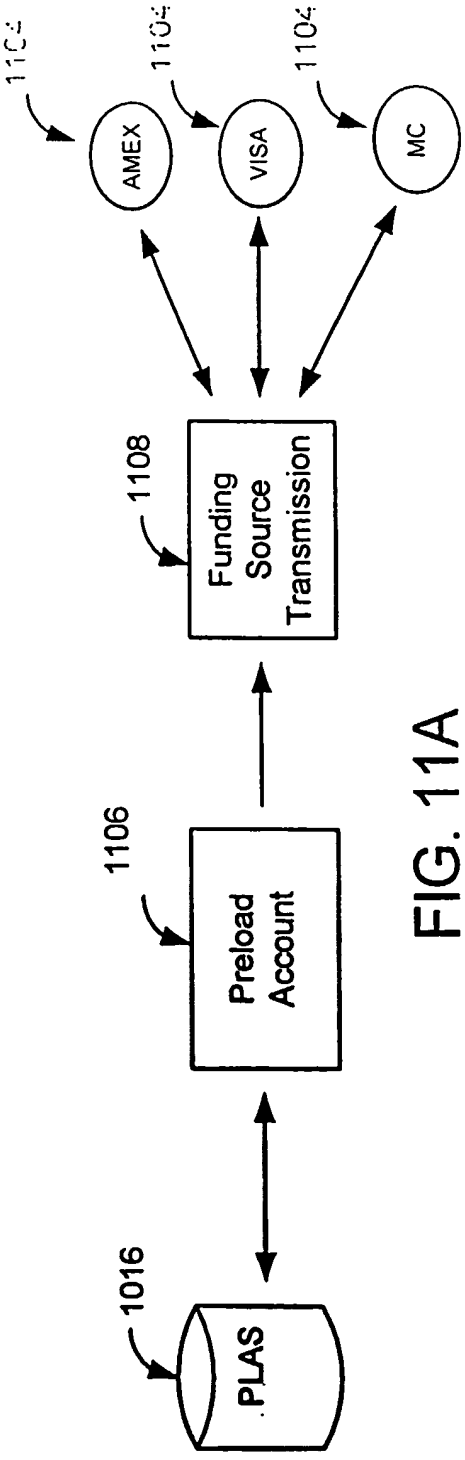


FIG. 11A

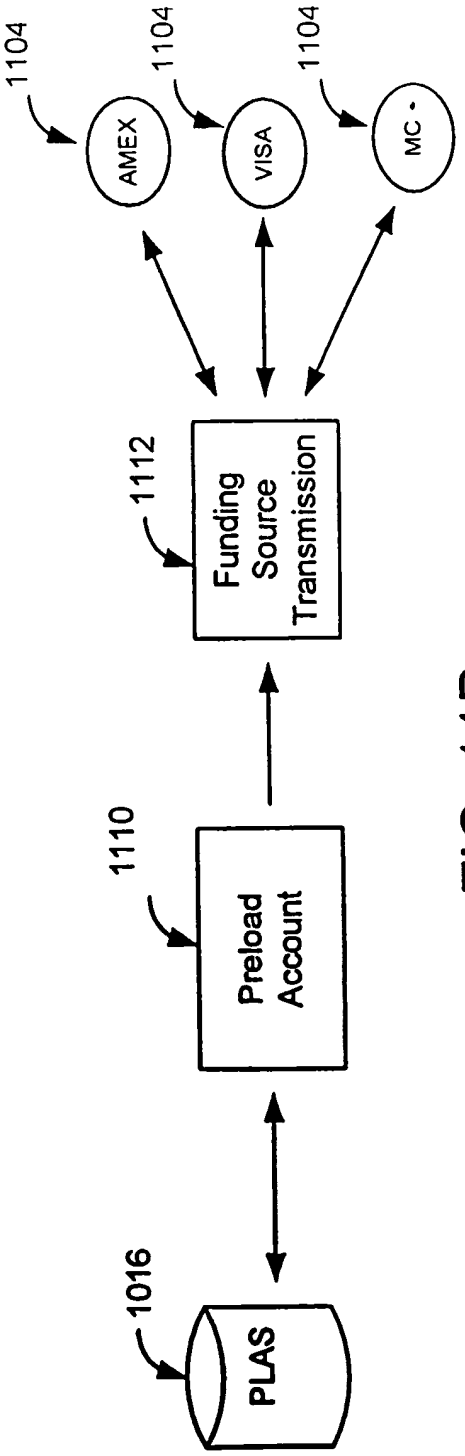


FIG. 11B

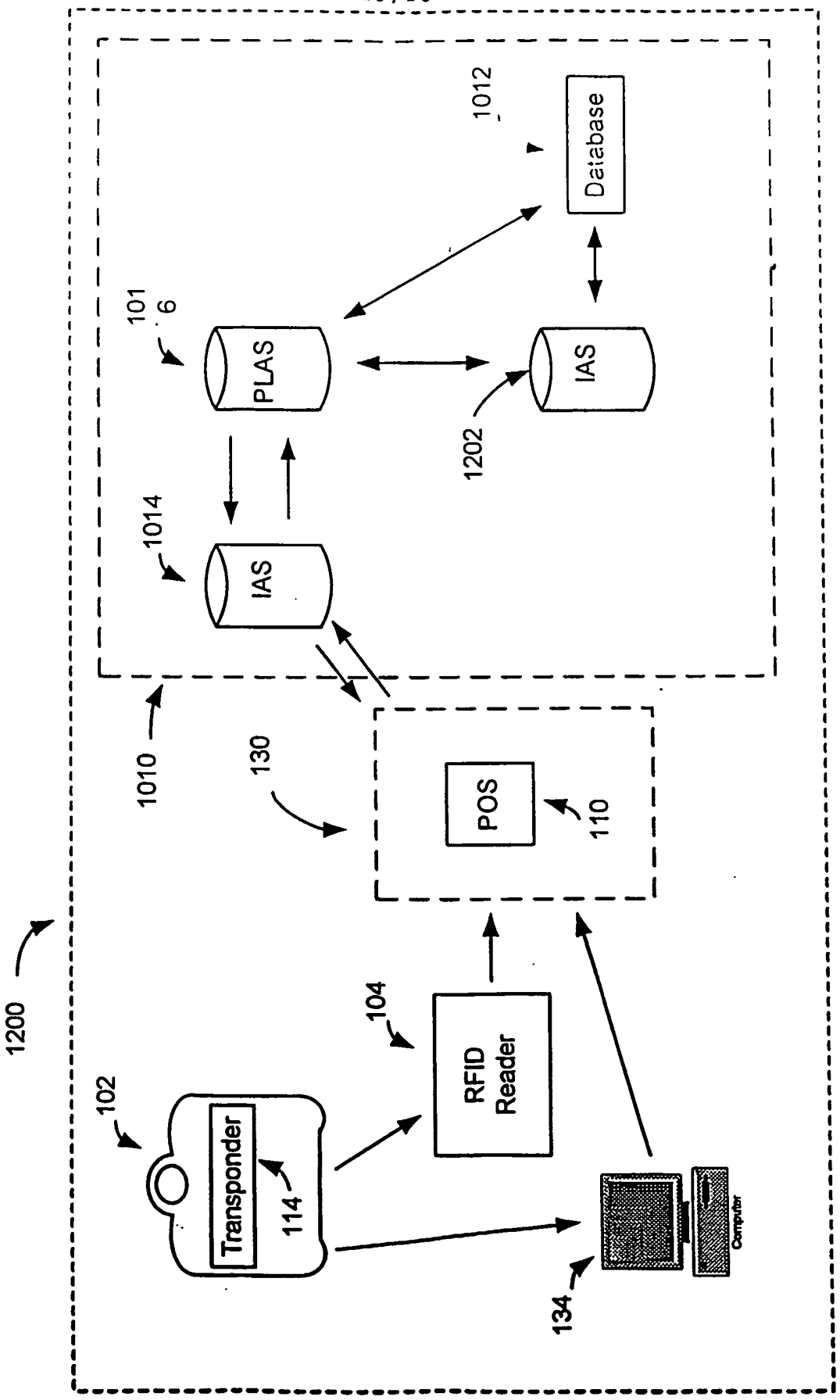

1200
1010
1012
Database
101
6
PLAS
IAS
1202
1014
IAS
130
POS
110
104
RFID
Reader
102
Transponder
114
134
Computer

FIG. 12

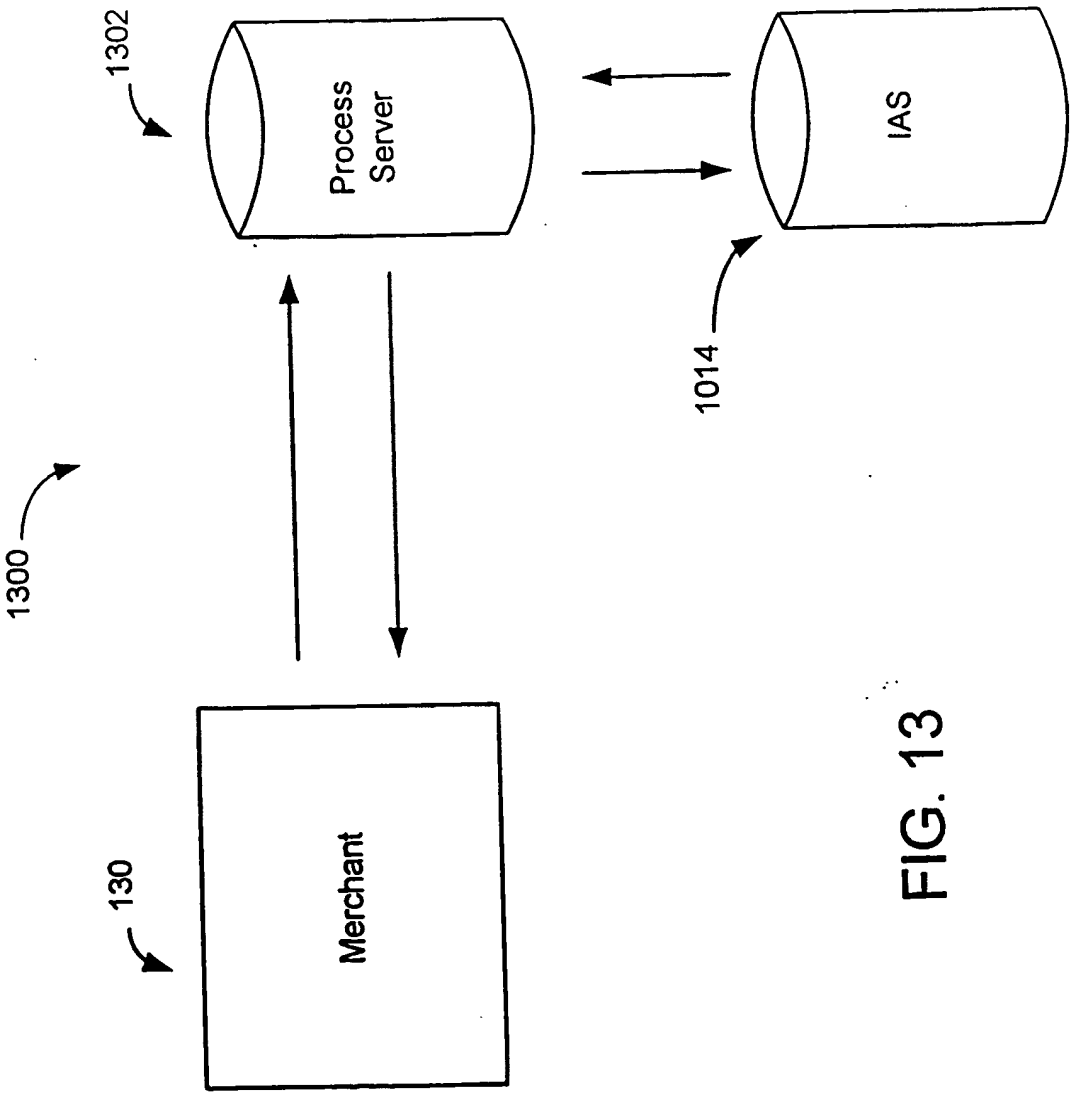


FIG. 13